明　細　書

情報処理サーバ及び情報処理方法

技術分野

本発明は、いつでもどこでも情報通信を行える、いわゆる「ユビキタス」通信環境下において、個人情報を保護しながら電子商取引を行う技術に係り、特に認証情報を利用した情報処理方法、及びこの情報処理方法に用いる情報処理サーバに関する。更には、異機種間の通信端末での画像情報の通信の互換性等を実現するための技術に関する。

背景技術

現在、インターネットと携帯端末の普及によりいつでもどこでも情報通信を行えるようになってきている。そのため通信される情報が他人に漏れないように様々な暗号化が考えられており、暗号化されたＨＴＴＰＳ（Hypertext Transfer Protocol Security）などのプロトコルを利用して情報をサーバに送信することも頻繁に行われている。そのため通信される情報が他人に漏れないように様々な暗号化が考えられている。暗号化方式にも秘密鍵方式や公開鍵方式等が利用されている。発信者から受信者まで単純に情報が伝達される場合、発信者と受信者の間で暗号化鍵を決めておけば暗号を解読されな

い限りそれ程問題とはならない。しかし電子商取引等では、個人情報を認証するサーバと実際に商取引を行うサーバが異なることがほとんどである。更にネットワークが複雑になり、種々の情報を同時にやり取りするようになると処理に係わるサーバの数は多くなる。したがって全情報を一括して暗号化してしまうと、途中のサーバで全情報を復号する必要が生じ、サーバに不必要な情報までもが知られてしまうことになる。この様に複数のサーバで処理される情報を、必要な部分のみ参照できるようにして情報を保護する方法はまだ考えられていない。

携帯端末の場合、規格が通信事業者によって決まるため、例えば、携帯端末を識別する機器識別子を取得することにより、サーバは携帯端末の認証を高い精度で行うことができるが、インターネット等の通信ネットワークにおいて、コンピュータ等の認証を行うことは困難とされている。即ち、コンピュータでインターネット等に接続するために利用するブラウザやＨＴＴＰ（Hypertext Transfer Protocol）などのプロトコルによれば、携帯端末の様に、コンピュータを識別する識別子を取得しサーバに送信することが不可能である。実際は、ブラウザのクッキーにサーバが作成した暗号化された暗号文を記憶し、認証時にその暗号文をサーバに送信したり、サーバへの接続時にユーザにパスワードを入力させるなどの方法が一般的である。

特開２００３－６１６４号公報に開示されているよ

うに、Ｗｅｂ上の提携サイトとネットワークを介して接続され、提携サイトへのアクセスが許容されたユーザの認証情報を格納するユーザ情報データベースと、提携サイトへ入力された認証情報を取得し、ユーザ情報データベースに基づいて認証処理を行い、認証結果を提携サイトへ送信する制御手段（モジュール）とを備えた認証システムなどがある。

又、二次元コード読取機能付き通信端末が開発され、二次元コード画像化された情報を通信端末に取り込むことが可能となった。更に、一部の通信端末には、二次元コード生成機能が内蔵されている。これにより通信端末の画面上に、情報を二次元コード化した画像を表示し、その画像を他の通信端末で読み取ることにより，通信端末間で情報の受け渡しが可能となってきている（後藤祥子、“ZDNet/JAPAN”、[online]、２００３年７月１５日、[平成１５年９月２２日検索]、インターネット<ＵＲＬ；
http://www.zdnet.co.jp/mobile/0307/15/n_qrprint.html>参照。）。

発明の開示

ユビキタスコンピューティングでは、必ずしもパーソナルコンピュータや携帯電話を必要としない。一般的にユビキタスコンピューティングは、加入者識別手段（モジュール）（ＳＩＭ）カード、ＩＣチップ又は無線タグ

（ＲＦＩＤ）等からなる自動認識タグとウェアラブルコンピュータと複数のサーバからなるメタサーバによって実現される。この様な環境下では、セキュリティ及び個人情報の保護が非常に重要になってくる。特にウェアラブルコンピュータでは、第３者に絶対に知られたくない情報をユーザが持ち歩く可能性があるため、こうした個人情報を送信する際、第３者に知られることなく、安全に当事者間での情報の送受信が行われるシステムの実現が重要となってきている。しかしながら、ユビキタス環境下における次世代ウェアラブルコンピュータによる通信において、個人情報保護の技術について標準的な方法は存在しない。又、ウェアラブルコンピュータのメモリ領域に記憶される情報量も増加の傾向にあり、メモリ容量が不足するという問題があった。

しかし上述した特開２００３－６１６４号公報に開示された発明においては、認証システムにおいてのみ認証されれば、複数の提携サイトについての認証は必要ないが、認証システムにおける認証において盗聴された場合、ユーザの損失は計り知れないものがある。

一方、携帯電話機などの携帯端末の普及に伴い、携帯電話を利用して様々なサービスを享受するユーザが多く、サービスの提供時には氏名、住所などの個人情報を登録する場合がある。この場合、入力するユーザインターフェースに乏しい携帯端末においてこれらの個人情報を登録するのは非常に困難であり、コンピュータでの登録を

望むユーザも多い。しかしコンピュータでの登録においては、上述したようなユーザ認証時の問題があり、これを打破するシステムの開発が望まれている。

情報の二次元コード化の記述方式が通信端末の機種によって異なるため、異機種間の通信端末では、画像を読み取れたとしてもデータ形式が崩れてしまう。したがって、通信端末の機能を十分に生かすためには、出力側と読取側が同機種でなければいけない。そのため、機種間の互換性を実現するシステムの開発が望まれている。

本発明は、ユビキタス環境下における次世代ウェアラブルコンピュータによる通信において、個人情報等のデータを当事者以外から秘匿しながら電子商取引を可能とする情報処理方法、及びこの情報処理方法に用いる情報処理サーバを提供することを目的とする。

上記目的を達成するため、本発明の第１の特徴は、認証端末が備える認証情報を利用して、認証情報を備えない通信端末を認証する情報処理システムに用いられる情報処理サーバに関する。即ち、本発明の第１の特徴に係る情報処理サーバは、（ａ）認証情報を記憶した認証情報記憶装置；（ｂ）通信端末の認証依頼を受信する；（ｃ）認証パラメータを生成し、認証パラメータを含む認証画像を生成して通信端末に送信し、認証パラメータを認証

パラメータ記憶装置に記憶する認証画像生成モジュール；（ｄ）通信端末から取得した認証画像の情報；（ｅ）認証端末が備える認証情報を、認証端末から取得する認証情報取得モジュール；（ｆ）認証パラメータ記憶装置を参照して、認証情報取得モジュールで取得した認証画像の情報が、認証画像生成モジュールで生成された画像の情報であり、更に、認証端末が備える認証情報が、認証情報記憶装置に記憶した認証情報と一致するか否かを判定し、その結果を通信端末に送信する認証情報照合モジュールとを備えることを要旨とする。

本発明の第２の特徴は、認証端末が備える認証情報を利用して、認証情報を備えない通信端末を認証する情報処理システムに用いられる情報処理方法に関する。即ち、本発明の第２の特徴に係る情報処理方法は：

（ａ）認証情報を認証情報記憶装置に記憶するステップ；

（ｂ）認証画像生成モジュールによって、通信端末の認証依頼を受信する；

（ｃ）認証パラメータを生成し、認証パラメータを含む認証画像を生成して通信端末に送信し、認証パラメータを認証パラメータ記憶装置に記憶する認証画像を生成するステップ；

（ｄ）認証情報取得モジュールによって、認証端末から、通信端末から取得した認証画像の情報；

（ｅ）認証端末が備える認証情報を取得するステップ；

（ｆ）認証情報照合モジュールによって、認証パラメータ記憶装置を参照して、認証画像の情報が、認証画像を生成するステップで生成された画像の情報であり、更に、認証端末が備える認証情報が、認証情報記憶装置に記憶した認証情報と一致するか否かを判定し、その結果を通信端末に送信する認証情報を照合するステップ

とを含むことを要旨とする。

本発明の第３の特徴は、通信端末識別子によって検索される対応情報を格納する識別子対応情報記憶装置と、通信端末から入力される情報を、対応情報に従って変換する情報変換モジュールとを備える情報処理サーバであることを要旨とする。

本発明の第４の特徴は、第１端末、第２端末、及び第１端末と第２端末間を仲介する情報処理サーバとを含むシステムを用いた情報処理方法に関する。即ち、本発明の第４の特徴に係る情報処理方法においては、情報処理サーバが：

（ａ）第１端末からのアクション要求を、第１レベルの個人情報と共に受信し、

（ｂ）第１レベルの個人情報により、第１端末を認証し、

（ｃ）第１端末に認証情報を発行し、

（ｄ）第１レベルの個人情報よりもセキュリティレベルの高い第２レベルの個人情報を、認証情報と共に第１端末から受信し、

（ｅ）認証情報に基づき、アクションに第２レベルの個人情報を第２端末に送信する

ことを要旨とする。

図面の簡単な説明

図１は、本発明の第１の実施例に係る情報処理システムを説明するデータフロー図である。

図２は、本発明の第１の実施例に係る情報保護方式における第１の暗号化鍵取得システムを説明するデータフロー図である。

図３は、本発明の第１の実施例に係る情報保護方式における第２の暗号化鍵取得システムを説明するデータフロー図である。

図４は、本発明の第２の実施例に係る電子商取引における情報処理システムを説明するデータフロー図である。

図５は、本発明の第３の実施例に係るコミュニティ内の情報交換における情報処理システムを説明するデータフロー図である。

図６は、本発明の第４の実施例に係る暗号化鍵取得システムを説明するデータフロー図である。

図７は、本発明の第４の実施例に係る暗号化鍵取得方法を示すフローチャートである。

図８は、本発明の第５の実施例に係る暗号化鍵取得方法を示す模式図である。

図９は、本発明の第５の実施例に係る暗号化鍵取得方法を示すフローチャートである。

図１０は、本発明の第６の実施例に係る暗号化鍵取得方法を示す模式図である。

図１１は、本発明の第６の実施例に係る暗号化鍵取得方法を示すフローチャートである。

図１２は、本発明の第７の実施例に係る情報処理サーバの機能ブロック図と、情報処理サーバが用いられる情報処理システムのシステム構成図である。

図１３は、本発明の第７の実施例に係る情報処理方法を示すシーケンス図である。

図１４は、本発明の第８の実施例に係る情報処理サーバの機能ブロック図と、情報処理サーバが用いられる情報処理システムのシステム構成図である。

図１５は、本発明の第８の実施例に係る情報処理方法を示すシーケンス図である。

図１６は、本発明の第８の実施例の変形例に係る情報処理方法を示すシーケンス図である。

図１７は、本発明の第９の実施例に係る情報処理サーバの機能ブロック図と、情報処理サーバが用いられる情報処理システムのシステム構成図である。

図１８は、本発明の第９の実施例に係る情報処理サーバがユーザに提示する質問リストとそのセレクトリストの一例である。

図１９は、関連技術のパスワードによる認証の場合の組合せを示した図である。

図２０は、本発明の第９の実施例に係る情報処理方法を示すシーケンス図である。

図２１は、本発明の第１０の実施例に係る情報処理サーバの機能ブロック図と、情報処理サーバが用いられる情報処理システムのシステム構成図である。

図２２は、本発明の第１０の実施例に係る情報処理方法を示すシーケンス図である。

図２３は、本発明の第１１の実施例に係る情報処理サーバの機能ブロック図と、情報処理サーバが用いられる情報処理システムのシステム構成図である。

図２４は、本発明の第１１の実施例に係る通信許可時の情報処理方法を示すシーケンス図である。

図２５は、本発明の第１１の実施例に係る通信不許可時の情報処理方法を示すシーケンス図である。

図２６は、本発明の第１２の実施例に係る情報処理システムのシステム構成図である。

図２７は、本発明の第１２の実施例に係る情報処理方法を説明するフローチャートである。

図２８は、本発明の第１２の実施例に係る情報処理方法における情報処理サーバに着目したフローチャートで

ある。

図２９は、本発明の第１２の実施例の変形例に係る情報処理方法を説明するフローチャートである。

図３０は、本発明の第１２の実施例の他の変形例に係る情報処理方法の処理の流れを説明する模式図である。

図３１は、本発明の第１２の実施例の更に他の変形例に係る情報処理方法の処理の流れを説明する模式図である。

図３２は、本発明の第１２の実施例の更に他の変形例に係る情報処理方法の処理の流れを説明する模式図である。

図３３は、本発明の第１３の実施例に係る情報処理システムのシステム構成図である。

図３４は、本発明の第１３の実施例に係る情報処理方法を説明するフローチャートである。

図３５は、本発明の第１３の実施例に係る情報処理方法における情報処理サーバに着目したフローチャートである。

図３６は、本発明の第１４の実施例に係る情報処理システムのシステム構成図である。

図３７は、本発明の第１４の実施例に係る情報処理方法を説明するフローチャートである。

図３８は、本発明の第１４の実施例に係る情報処理方法における情報処理サーバに着目したフローチャートである。

図３９は、本発明の第１４の実施例の変形例に係る情報処理方法を説明するフローチャートである。

図４０は、本発明の第１４の実施例の他の変形例に係る情報処理方法の処理の流れを説明する模式図である。

図４１は、本発明の第１４の実施例の更に他の変形例に係る情報処理方法の処理の流れを説明する模式図である。

発明を実施するための最良の形態

次に、図面を参照して、本発明の第１乃至第１４の実施例を説明する。以下の図面の記載において、同一又は類似の部分には同一又は類似の符号を付している。但し、図面は模式的なものであり、比率等は現実のものとは異なることに留意すべきである。したがって、具体的な構造は以下の説明を参酌して判断すべきものである。又図面相互間においても互いの寸法の関係や比率が異なる部分が含まれていることは勿論である。

（第１の実施例）

本発明の第１の実施例に係る個人情報保護方式について、図１、図２及び図３を参照しながら説明する。図１で「Ｅｎ（Ｘ）」で表現しているものは、第ｎサーバによって復号できるように暗号化鍵によってＸというデータを暗号化して生成された情報を示している。例えば「Ｅ

３（ＤＡＴＡ１）」は、第２サーバ７４によって復号できるように暗号化鍵によってＤＡＴＡ１というデータを暗号化した情報となる。図１では例示的にｎ＝３として説明する。

まず、図１に示すユビキタスコンピューティングでは、ユーザが利用する第１のウェアラブルコンピュータとしての携帯情報端末１０ａと、第１のウェアラブルコンピュータ（携帯情報端末）１０ａから送信される送信元メタデータＭＤ０を処理する複数のサーバからなるメタサーバ７６と、データの送信先である送信先サーバＲ４０が存在する。ここでメタサーバ７６は、例示的に第１サーバ７２、第２サーバ７３、第２サーバ７４、送信サーバ２４のサーバ群と、各サーバを接続する第１の匿名通信路７１ａ、第２の匿名通信路７１ｂ、第３の匿名通信路７１ｃと、第２サーバ７３に接続された暗号化情報データベース２５から構成されているものとする。実際にはサーバ、通信路そしてデータベースの数には制限はない。「匿名通信路」とは、通信されるパケット情報が他人にのぞき見されないようにした通信路であり、ＬＡＮケーブル接続通信路、無線接続通信路、専用線接続通信路等のいずれであっても良い。

図１を参照しながら、情報保護方法について説明する

（ａ）第１のウェアラブルコンピュータ（携帯情報端末）１０ａで、第１サーバ７２によってのみ復号できる暗号化鍵で第１の情報ＤＡＴＡ３を暗号化し第１の暗号化情報Ｅ１（ＤＡＴＡ３）を生成し、第２サーバ７３によってのみ復号できる暗号化鍵で第２の情報ＤＡＴＡ２を暗号化し第２の暗号化情報Ｅ２（ＤＡＴＡ２）を生成し、第２サーバ７４によってのみ復号できる暗号化鍵で第３の情報ＤＡＴＡ１を暗号化し第３の暗号化情報Ｅ３（ＤＡＴＡ１）を生成し、メタサーバ７６は送信元メタデータＭＤ０として受信する。ＤＡＴＡ１、ＤＡＴＡ２、ＤＡＴＡ３、・・・・とは、例えば個人認証情報、端末情報、送信先情報、商品情報、メール情報、画像情報等の情報である。

（ｂ）送信元メタデータＭＤ０を受信した第１サーバ７２は、第１サーバ７２で処理に必要かつ復号できる情報を検出する。図１では、Ｅ１（ＤＡＴＡ３）があるので、これを復号してＤＡＴＡ３を得て処理を行う。その後、ＤＡＴＡ３を送信先サーバＲ４０で復号できるように再度暗号化してＥＲ（ＤＡＴＡ３）に置換する。そして第１送信メタデータＭＤ１を生成し、第１の匿名通信路７１ａを経由して第２サーバ７３に送信する。その他の情報は第１サーバ７２では復号できないため、第１サーバ７２に対しては秘匿されていることになる。なお、別のサーバで復号できるように暗号化するための暗号化鍵取得方法については、図２及び図３を参照しながら後

で詳述する。

（ｃ）第１送信メタデータＭＤ１を受信した第２サーバ７３は、第２サーバ７３で処理に必要かつ復号できる情報を検出する。図１では、Ｅ２（ＤＡＴＡ２）があるので、第１サーバ７２で行った方法と同様にして復号してＤＡＴＡ２を得て処理を行う（図示せず）。その後、ＤＡＴＡ２を送信先サーバＲ４０で復号できるように再度暗号化してＥＲ（ＤＡＴＡ２）に置換する。又、もう１つの処理として、第２サーバ７３では復号化して情報の内容を知ることができない情報を利用して、新たな情報を追加する。図１では、Ｅ３（ＤＡＴＡ１）は第２サーバ７４で復号されるものであるが、第２サーバ７３に接続された暗号化情報データベース２５の内容をこのＥ３（ＤＡＴＡ１）をキー情報として第ｎ＋１の暗号化情報Ｅ３（ＩＮＦＯ２）を得る。そしてＥ３（ＩＮＦＯ２）を追加して第２送信メタデータＭＤ２を生成し、第２の匿名通信路７１ｂを経由して第２サーバ７４に送信する。

（ｄ）第２送信メタデータＭＤ２を受信した第２サーバ７４は、第２サーバ７４で処理に必要かつ復号できる情報を検出する。図１では、Ｅ３（ＤＡＴＡ１）とＥ３（ＩＮＦＯ２）があるので、第１サーバ７２で行った方法と同様にして復号してＤＡＴＡ１とＩＮＦＯ２を得て処理を行う。その後、ＤＡＴＡ１とＩＮＦＯ２を送信先サーバＲ４０で復号できるように再度暗号化してＥＲ（ＤＡＴＡ１）とＥＲ（ＩＮＦＯ２）に置換する。そし

て第３送信メタデータＭＤ３を生成し、第３の匿名通信路７１ｃを経由して送信サーバ２４に送信する。

（ｅ）送信サーバ２４は送信先アドレスによって、第３送信メタデータＭＤ３をメタサーバ７６外の送信先サーバＲ４０に送信する。最終的な第３送信メタデータＭＤ３内の情報は送信先サーバＲ４０で復号できるように、経由してきた第１サーバ７２、第２サーバ７３及び第２サーバ７４で暗号化されている。

次に、別のサーバで復号できるように再暗号化するための暗号化鍵取得方法について説明する：

図２に示す暗号化鍵取得方法の実施例では、送信元メタデータＭＤ０を受信した第１サーバ７２は、Ｅ１（ＤＡＴＡ２）を復号化してＤＡＴＡ２を得る。つづいてＤＡＴＡ２を再度利用する別のサーバ用に暗号化するための鍵を得るために、別のサーバ情報を示すＥ３（ＤＡＴＡ１）（図２では暗号化された事業者情報）を検索キーとし、第１サーバ７２に接続された暗号化鍵データベース２５ａを検索し「Ｋｅｙ２」という暗号化鍵を取得する。そしてこの「Ｋｅｙ２」によってＤＡＴＡ２を暗号化しＥＲ（ＤＡＴＡ２）を生成し、第１送信メタデータＭＤ１とする。第１サーバ７２は、Ｅ３（ＤＡＴＡ１）をその情報のままで検索キーとして利用するだけで復号化することはできないため、ＤＡＴＡ１の内容は第１サーバ７２には秘匿される。

又、図３に示す暗号化鍵取得方法の別の実施例では、送信元メタデータＭＤ０を受信した第１サーバ７２は、Ｅ１（ＤＡＴＡ２）を復号化してＤＡＴＡ２を得る。つづいてＤＡＴＡ２を再度利用する別のサーバ用に暗号化するための鍵を得るために、別のサーバ情報を示すＥ３（ＤＡＴＡ１）のみを暗号化サーバ７７に送信する。暗号化サーバ７７では、Ｅ３（ＤＡＴＡ１）を復号してＤＡＴＡ１を得る。次にＤＡＴＡ１を検索キーとして暗号化鍵データベース２５ａを検索し「Ｋｅｙ２」という暗号化鍵を取得する。そしてこの「Ｋｅｙ２」によってＤＡＴＡ１を暗号化しＥＲ（ＤＡＴＡ１）を生成し第１サーバ７２に返信する。

第１サーバ７２はＥ３（ＤＡＴＡ１）をＥＲ（ＤＡＴＡ１）に置換する。もう１つの処理として、第１サーバ７２は暗号化サーバ７７から「Ｋｅｙ２」を受信してＤＡＴＡ２を暗号化してＥＲ（ＤＡＴＡ２）を生成する。

図３に示した実施例でも、Ｅ３（ＤＡＴＡ１）の内容であるＤＡＴＡ１は第１サーバ７２に秘匿になっている。又、暗号化サーバ７７にはＥ３（ＤＡＴＡ１）しか送信されないので、他の情報は暗号化サーバ７７に対して秘匿されている。

本発明の第１の実施例によれば、各サーバは、サーバの処理に必要な情報のみを復号化して知ることができる。他の情報については受信しても内容は秘匿されたままにできるため、メタサーバ７６内のサーバであっても不必要にのぞき見することはできない。したがって、個人情報等のセキュリティが確保され、安全にユビキタスコンピューティングを実現できる。

（第２の実施例）

本発明の第２の実施例に係る個人情報保護方式の具体例について、図４は、モバイル環境下でのウェアラブルコンピュータ（携帯情報端末）を用いたユビキタスコンピューティングにおける電子商取引の流れについて示している。図４に示す電子商取引システムは、第１のウェアラブルコンピュータ（携帯情報端末）１０ａと、個人認証サーバ２６、端末認証サーバ２７、事業者認証サーバ２８からなるメタサーバ７６と、個人認証サーバ２６と端末認証サーバ２７を接続する第１の匿名通信路７１ａ、端末認証サーバ２７と事業者認証サーバ２８を接続する第２の匿名通信路７１ｂ、商品提供事業者５０、そして商品提供事業者５０が保有する事業者サーバ５１からなる。

例示的な処理の流れは以下のようになる：

（ａ）まず第１のウェアラブルコンピュータ（携帯情報端末）１０ａより、個人情報、端末情報、事業者情報、商品情報等がメタサーバ７６に送信される。

（ｂ）個人認証サーバ２６は、受信したメタデータの内個人情報のみを復号化して、個人の正当性を認証する。個人認証サーバ２６はその他の情報については知ることができない。

（ｃ）次に端末認証サーバ２７は、第１の匿名通信路７１ａを経由して受信したメタデータの内端末情報のみを復号化して、端末の正当性を認証する。端末認証サーバ２７はその他の情報については知ることができない。

（ｄ）次に事業者認証サーバ２８は、第２の匿名通信路７１ｂを経由して受信したメタデータの内事業者情報のみを復号化して、事業者の正当性を認証する。事業者認証サーバ２８はその他の情報については知ることができない。

（ｅ）メタサーバ７６で必要な認証が完了すると、メタデータは商品提供事業者５０の保有する事業者サーバ５１へ送信される。事業者サーバ５１では、商取引に必要な、個人情報や商品情報を復号して読み取り確認すると、商品の送付を行い商取引が完了する。

本発明の第２の実施例によれば、図４に示した流れの中では、メタサーバ７６の個人認証サーバ２６、端末認証サーバ２７、事業者認証サーバ２８のいずれのサーバ

も、ユーザは何を購入したかを知ることはないし、どの商品提供事業者５０との間で商取引を行っているのかも知ることはない。この様に必要な認証を行いながらも、個人的な情報を秘匿したままで電子商取引を行うことができる。

（第３の実施例）

本発明の第３の実施例に係る個人情報保護方式の具体例について、図５は、モバイル環境下でのコミュニティにおける情報交換の流れについて示している。図５に示す情報交換システムは、第１のウェアラブルコンピュータ（携帯情報端末）１０ａと第２のウェアラブルコンピュータ（携帯情報端末）１０ｂ、個人認証サーバ２６、送付先認証サーバ２９からなるメタサーバ７６と、個人認証サーバ２６と送付先認証サーバ２９の間に設けられた第１の匿名通信路７１ａからなる。

例示的な処理の流れは以下のようになる：

（ａ）第１のウェアラブルコンピュータ（携帯情報端末）１０ａ（会員Ａ）から、以下の情報を含む送信元メタデータＭＤ０を送信する。

(i)個人認証サーバ２６で復号できる形に暗号化した会員Ａ情報

(ii)送付先認証サーバ２９で復号できる形に暗号化

した会員Ｂのアドレス

(iii)第２のウェアラブルコンピュータ(携帯情報端末)１０ｂ(会員Ｂ)で復号できる形に暗号化した秘密のメッセージ

(ｂ)メタサーバ７６の個人認証サーバ２６が、受信した送信元メタデータＭＤ０の中の会員Ａ情報を復号化して個人認証を行う。その後、会員Ａ情報を第２のウェアラブルコンピュータ１０ｂで復号できる形に再暗号化して置換する。そして生成されたメタデータを送付先認証サーバ２９に送信する。

(ｃ)送付先認証サーバ２９は、第１の匿名通信路７１ａを経由してメタデータを受信する。そして送付先認証サーバ２９で復号できる形に暗号化された会員Ｂのアドレスを復号し、会員Ｂがコミュニティの一員であるかどうかを認証する。正しく認証できた場合、送付先認証サーバ２９は第２のウェアラブルコンピュータ１０ｂに向かってメタデータを送信する。

(ｄ)第２のウェアラブルコンピュータ１０ｂは受信したメタデータを復号して受信復号メタデータＭＤ４を生成し、会員Ａ情報と秘密のメッセージを表示又は音声等でユーザに通知する。

本発明の第３の実施例によれば、メタサーバ７６の個人認証サーバ２６で送信元を認証し、送付先認証サーバ２９で送信先を認証するので、閉じられたコミュニティ

の会員同士の間に情報交換を限定することができる。この様に外部の人からの発言を阻止できる上に、誤って外部の人に情報が送信され読まれてしまうことも防止できる。又、個人認証サーバ２６は、送信相手が誰なのかを知ることはないし、送付先認証サーバ２９は送信元が誰なのかを知ることはない。よって、閉じられたメタサーバ７６のサーバ同士でも個人間の情報を互いに秘匿状態にしたままやり取りができるので、個人情報の保護に優れている。

（第４の実施例）

本発明の第４の実施例に係る暗号化鍵取得システムは、図６に示すように、ユーザが利用する第１のウェアラブルコンピュータ（携帯情報端末）１０ａと、第１のウェアラブルコンピュータ１０ａから送信される送信元メタデータＭＤ０を処理する第１サーバ７２と、第１サーバ７２に接続された暗号化鍵データベース２５ａから構成される。但し、第１サーバ７２は、複数のサーバからなるメタサーバの内のサーバの任意の１つとして説明する。

次に、図７を参照しながら本発明の第４の実施例に係る暗号化鍵取得方法について例示的な処理の流れを説明する：

（ａ）まず、ステップＳ１０１において、第１のウェ

アラブルコンピュータ１０ａのメモリ内に格納された固定乱数ＲＮにより生成される検索タグ情報ＣＯＤＥを暗号化した暗号化検索タグ情報Ｅ（ＣＯＤＥ）を含む送信元メタデータＭＤ０を第１サーバ７２が受信する。

（ｂ）次に、ステップＳ１０２において、送信元メタデータＭＤ０から暗号化検索タグ情報Ｅ（ＣＯＤＥ２）を検索する。

（ｃ）ステップＳ１０２において、暗号化検索タグ情報Ｅ（ＣＯＤＥ２）が検出されない場合は、ステップ１０５において、第１送信メタデータを次段以降のサーバに送信する。

（ｄ）一方、ステップＳ１０２において、暗号化検索タグ情報Ｅ（ＣＯＤＥ２）が検出されると、ステップ１０３において、検索タグ情報ＣＯＤＥ２にあらかじめ関連づけられる関連情報である暗号化鍵データＫｅｙ２が暗号化鍵データベース２５ａから第１サーバ７２へ送信される。次に、第１サーバ７２は、Ｅ１（ＤＡＴＡ２）を復号化してＤＡＴＡ２を処理後、ステップ１０４において、ＤＡＴＡ２を「Ｋｅｙ２」によってサーバＲで読み取りが可能な情報に暗号化しＥＲ（ＤＡＴＡ２）を生成し、第１送信メタデータＭＤ１内に格納する。次に、ステップ１０５において、第１サーバ７２は、第１送信メタデータＭＤ１を次段以降のサーバに転送する。

図６で示す「ＣＯＤＥ２」は検索タグ情報であり、第

１のウェアラブルコンピュータ１０ａに搭載されるメモリ領域に記録された固定乱数ＲＮを用いて生成される。固定乱数ＲＮは、ウェアラブルコンピュータ毎毎に特徴のある固有のデータであり、例えば８ビット、１６ビット、３２ビット６４ビット等の特定の大きさを有する。固定乱数ＲＮは、検索タグ情報ＣＯＤＥ２としてそのまま用いることも可能であるが、第１のウェアラブルコンピュータ１０ａの内部に記録される住所、電話番号、日付、時刻、氏名等の第１のウェアラブルコンピュータ１０ａに内蔵される情報を用いて加工されたデータであっても良い。「Ｅ（ＣＯＤＥ２）」は検索タグ情報を暗号化したデータである。検索タグ情報ＣＯＤＥ２を暗号化する手段（モジュール）としては、住所、電話番号、日付、時刻、氏名等の第１のウェアラブルコンピュータ１０ａに内蔵される情報を用いて乱数を発生させることも可能である。

本発明の第４の実施例によれば、各サーバは、サーバの処理に必要な情報のみを復号化して知ることができる。他の情報については受信しても内容は秘匿されたままにできるため、メタサーバ７６内のサーバであっても不必要にのぞき見することはできない。したがって、個人情報等のセキュリティが確保され、安全にユビキタスコンピューティングを実現できる。更に、固定乱数ＲＮは、受信サーバ側で初めて意味のあるデータに変換されるため、より秘匿性を高めることができる。又、必要な個人

情報がサーバ側で管理されることと、固定乱数ＲＮのデータサイズが小さくて済むため、第１のウェアラブルコンピュータ１０ａ内の使用メモリ領域を節約することが可能となる。

（第５の実施例）

本発明の第５の実施例に係る暗号化鍵取得システムは、図８に示すように、ユーザが利用する第１のウェアラブルコンピュータ（携帯情報端末）１０ａと、第１のウェアラブルコンピュータ１０ａから送信される送信元メタデータＭＤ０を処理する第１サーバ７２と、第１サーバ７２に接続された暗号化情報データベース２５から構成される。但し、第１サーバ７２は、複数のサーバからなるメタサーバの内のサーバの任意の１つとして説明する。

次に、図９を参照しながら本発明の第５の実施例に係る暗号化鍵取得方法について例示的な処理の流れを説明する：

（ａ）まず、ステップＳ１１１において、第１のウェアラブルコンピュータ１０ａのメモリ内に格納された固定乱数ＲＮにより生成される検索タグ情報ＣＯＤＥを暗号化した暗号化検索タグ情報Ｅ（ＣＯＤＥ）を含む送信元メタデータＭＤ０を第１サーバ７２が受信する。

（ｂ）次に、ステップＳ１１２において、送信元メタデ

ータＭＤ０から暗号化検索タグ情報Ｅ（ＣＯＤＥ２）を検索する。

（ｃ）ステップＳ１１２において、暗号化検索タグ情報Ｅ（ＣＯＤＥ２）が検出されない場合は、ステップ１１４において、第１送信メタデータＭＤ１を次段以降のサーバに送信する。

（ｄ）一方、ステップＳ１１２において、暗号化検索タグ情報Ｅ（ＣＯＤＥ２）が検出されると、ステップ１１３において、検索タグ情報ＣＯＤＥ２にあらかじめ関連づけられた関連情報である暗号化情報Ｅ２（ＩＮＦＯ２）が第１送信メタデータＭＤ１に格納される。次に、ステップＳ１１４において、第１送信メタデータＭＤ１は次段以降のサーバに転送される。但し、暗号化情報Ｅ２（ＩＮＦＯ２）は２段目のサーバで読取りが可能な暗号化情報データであるが、他のサーバの処理に必要な情報であっても良い。

本発明の第５の実施例によれば、各サーバは、サーバの処理に必要な情報のみを復号化して知ることができる。他の情報については受信しても内容は秘匿されたままにできるため、メタサーバ７６内のサーバであっても不必要にのぞき見することはできない。したがって、個人情報等のセキュリティが確保され、安全にユビキタスコンピューティングを実現できる。更に、固定乱数ＲＮは、受信サーバ側で初めて意味のあるデータに変換されるた

め、より秘匿性を高めることができる。又、必要な個人情報がサーバ側で管理されることと、固定乱数ＲＮのデータサイズが小さくて済むため、第１のウェアラブルコンピュータ１０ａ内の使用メモリ領域を節約することが可能となる。

（第６の実施例）

本発明の第６の実施例に係る暗号化鍵取得システムは、図１０に示すように、ユーザが利用する第１のウェアラブルコンピュータ（携帯情報端末）１０ａと、第１のウェアラブルコンピュータ１０ａから送信される送信元メタデータＭＤ０を処理する第１サーバ７２と、第１サーバ７２に接続された暗号化情報データベース２５から構成される。但し、第１サーバ７２は、複数のサーバからなるメタサーバの内のサーバの任意の１つとして説明する。ここでは、図８に示す「Ｅ１（ＤＡＴＡ２）」をサービス情報として説明する。サービス情報は、商品やサービスの取引において必要な情報が含まれ、例えばサイズ、色等の商品情報、事業者情報、配送情報などが考えられる。

次に、図１１を参照しながら本発明の第６の実施例に係る暗号化鍵取得方法について例示的な処理の流れを説明する：

（ａ）まず、ステップＳ１２１において、サービス情報を暗号化した暗号化情報Ｅ１（ＤＡＴＡ２）、及び第１のウェアラブルコンピュータ１０ａのメモリ内に格納された固定乱数ＲＮにより生成される検索タグ情報ＣＯＤＥ２を暗号化した暗号化検索タグ情報Ｅ（ＣＯＤＥ２）を含む送信元メタデータＭＤ０を第１サーバ７２が受信する。但し、サービス情報としては、２次元にコード化された情報等を第１のウェアラブルコンピュータ１０ａが光学的に読込むことで取得したデータ等が考えられる。

（ｂ）次に、ステップＳ１２２において、送信元メタデータＭＤ０から暗号化情報及び暗号化検索タグ情報を検索する。

（ｃ）次に、ステップＳ１２２において、暗号化情報Ｅ１（ＤＡＴＡ２）が検出された場合は、暗号化情報Ｅ１（ＤＡＴＡ２）にあらかじめ関連づけられる第２データ変換テーブル４２が選択される。次に、ステップＳ１２４において、第１サーバ７２は、ステップＳ１２４において、送信元メタデータＭＤ０から暗号化検索タグ情報を検索する。一方、暗号化情報Ｅ１（ＤＡＴＡ２）が検出されない場合は、そのまま第１サーバ７２は、ステップＳ１２４において送信元メタデータＭＤ０から暗号化検索タグ情報を検索する。

（ｄ）ステップＳ１２４において、暗号化検索タグ情報Ｅ（ＣＯＤＥ２）が検出されない場合は、ステップ１２６において、第１送信メタデータＭＤ１を次段以降の

サーバに送信する。

（ｅ）一方、ステップＳ１２４において、暗号化検索タグ情報Ｅ（ＣＯＤＥ２）が検出されると、ステップ１２５において、検索タグ情報ＣＯＤＥ２にあらかじめ関連づけられた関連情報である暗号化情報Ｅ２（ＩＮＦＯ２）が第１送信メタデータＭＤ１に格納される。次に、ステップＳ１２６において、第１送信メタデータＭＤ１は次段以降のサーバに転送される。

本発明の第６の実施例によれば、各サーバは、サーバの処理に必要な情報のみを復号化して知ることができる。他の情報については受信しても内容は秘匿されたままにできるため、メタサーバ７６内のサーバであっても不必要にのぞき見することはできない。したがって、個人情報等のセキュリティが確保され、安全にユビキタスコンピューティングを実現できる。

又、図１に示すユビキタスコンピューティングにおける個人情報保護方法が、個人情報、端末情報、事業者情報、商品情報等からなる送信元メタデータＭＤ０をメタサーバ７６に転送していたのに対し、ウェアラブルコンピュータ１０ａ側で生成された検索タグ情報ＣＯＤＥ２を扱うため、個人情報、端末情報、事業者情報、商品情報等からなる送信元メタデータＭＤ０をウェアラブルコンピュータ１０ａ内に保存する必要がなくなり、ウェアラブルコンピュータ１０ａの内部で使用されるメモリ領

域を節約することができる。

（第７の実施例）

図１２を参照して、本発明の第７の実施例に係る情報処理サーバ３０と、情報処理サーバ３０を利用した情報処理システムについて説明する。情報処理サーバ３０は、中央処理制御装置、メモリなどを備える一般的なコンピュータに所定の処理を実行するソフトウェアプログラムをインストールすることによって実現される。

本発明の情報処理サーバ３０は、第２通信端末（認証端末）２０ｂが備える認証情報を利用して、認証情報を備えない第１通信端末２０ａを認証する。ここで、第１通信端末２０ａは、一般的なコンピュータで、第２通信端末（認証端末）２０ｂは、認証情報を備えた携帯電話機などの通信端末である。認証情報は、指紋認証情報なのでも良いが、第７の実施例においては、情報処理サーバ３０が発行した暗号化され改竄不可能な認証識別子であるとする。

第７の実施例に係る情報処理システムにおいて、情報処理サーバ３０は、第１通信ネットワーク７０ａを介して第１通信端末２０ａと互いに接続可能で、更に、第２通信ネットワーク７０ｂを介して第２通信端末（認証端末）２０ｂと互いに接続可能である。第１通信ネットワーク７０ａと第２通信ネットワーク７０ｂは、少なくと

も一部が互いに交差しない通信ネットワークである。

第７の実施例に係る情報処理サーバ３０は、認証パラメータ記憶装置１０１、認証情報記憶装置１０２、認証識別子記憶装置３０２ｂ、画像生成手段（モジュール）３２、認証情報取得手段（モジュール）１１２、認証情報照合手段（モジュール）１１３、入出力制御手段（モジュール）３１を備えている。

認証識別子記憶装置３０２ｂは、情報処理サーバ３０が発行した第２通信端末（認証端末）２０ｂを認証するための認証識別子（認証情報）を記憶した記憶装置である。

画像生成手段（モジュール）３２は、第１通信端末２０ａの認証依頼を受信すると、認証パラメータを生成し、認証パラメータを含む認証画像を生成して第１通信端末２０ａに送信し、認証パラメータを認証パラメータ記憶装置１０１に記憶させる手段である。

ここで、画像生成手段（モジュール）３２で生成し、認証パラメータ記憶装置１０１に記憶される認証パラメータは、一意に特定できるワンタイムパスワードの様な乱数及び日時のいずれか１つ以上を含む情報である。この認証パラメータの「日時」は、認証パラメータ生成時の日時でも良いし、第１通信端末２０ａの認証依頼を受信した日時でも良い。又、認証パラメータ記憶装置１０１には、認証パラメータを有効にする期限である有効日時も記憶していても良い。画像生成手段（モジュール）

３２は、第１通信ネットワーク７０ａを介して第１通信端末２０ａに認証画像を送信する。ここでは認証画像を送信すると記載したが、第２通信端末（認証端末）２０ｂにおいて情報を解読できれば、テキストでも構わない。テキストの場合、簡単に盗聴できないような桁数の多いものが好ましい。

認証情報取得手段（モジュール）１１２は、第１通信端末２０ａから取得した認証画像の情報と、第２通信端末（認証端末）２０ｂが備える認証情報を、第２通信端末（認証端末）２０ｂから取得し、認証情報記憶装置１０２に記憶させる手段である。認証情報取得手段（モジュール）１１２は、第２通信ネットワーク７０ｂを介して第２通信端末（認証端末）２０ｂから認証情報を受信する。ここで、認証画像の情報は、第１通信端末２０ａから取得した認証画像を、第２通信端末（認証端末）２０ｂにおいてデコードした情報であっても良いし、第１通信端末２０ａから取得し、第２通信端末（認証端末）２０ｂから受信した認証画像を、情報処理サーバ３０においてデコードした情報であっても良い。更に、第１通信端末２０ａから認証画像の情報を取得する場合、第２通信端末（認証端末）２０ｂによって、第１通信端末２０ａに提示された認証画像を撮影しデコードしても良い。又、第１通信端末２０ａと第２通信端末（認証端末）２０ｂの間で赤外線通信などの近距離無線通信を利用したり、リムーバブルディスクを利用して、第２通信端末（認

証端末）２０ｂは認証画像を取得しても良い。

認証情報照合手段（モジュール）１１３は、認証パラメータ記憶装置１０１と認証情報記憶装置１０２と認証識別子記憶装置３０２ｂを参照して、認証情報取得手段（モジュール）１１２で取得した認証画像の情報が、画像生成手段（モジュール）３２で生成された画像の情報であり、更に、第２通信端末（認証端末）２０ｂが備える認証情報が、認証識別子記憶装置３０２ｂに記憶した認証情報と一致するか否かを判定し、その結果を第１通信端末２０ａに送信する手段である。更に、認証パラメータ記憶装置１０１において、認証パラメータの有効日時が記憶されている場合、認証情報取得手段（モジュール）１１２で取得した日時が、認証パラメータ記憶装置１０１に記憶された認証パラメータの有効日時以前の場合に認証を許可し、認証パラメータの有効日時以降の場合に認証を不可にしても良い。

入出力制御手段（モジュール）３１は、情報処理サーバ３０の入力や出力を制御し、それぞれのネットワークや手段(モジュール)にその情報を伝達する手段である。

第７の実施例に係る第１通信端末２０ａは、画像データ記憶装置１２ａ、画像取込手段(モジュール)１１ａ、認証画像提示手段（モジュール）２１２、認証結果取得手段（モジュール）２１３を備えている。

画像取込手段（モジュール）１１ａは、情報処理サーバ３０の画像生成手段（モジュール）３２によって生成

された認証画像を取得し、画像データ記憶装置１２ａに記憶させる手段である。　認証画像提示手段（モジュール）２１２は、画像データ記憶装置１２ａに記憶された認証画像データを第２通信端末（認証端末）２０ｂに提示する手段である。

更に、認証結果取得手段（モジュール）２１３は、情報処理サーバ３０の認証情報照合手段（モジュール）１１３によって送信された認証の結果を取得する手段である。

第７の実施例に係る第２通信端末（認証端末）２０ｂは、画像データ記憶装置１２ｂ、認証識別子記憶装置３０２ａ、画像取込手段（モジュール）３１１、認証情報送信手段（モジュール）３１２を備えている。

画像取込手段（モジュール）３１１は、第１通信端末２０ａの認証画像提示手段（モジュール）２１２によって提示された画像を撮影し、画像データ記憶装置１２ｂに記憶させる手段である。画像を撮影する必要はなく、第１通信端末２０ａに送信された認証画像を第２通信端末（認証端末）２０ｂに取得できればどのような手段（モジュール）を用いても構わない。

認証情報送信手段（モジュール）３１２は、認証識別子記憶装置３０２ａに記憶された、情報処理サーバ３０から取得した認証識別子と、画像データ記憶装置１２ｂに記憶された画像の情報を第２通信ネットワーク７０ｂを介して情報処理サーバ３０に送信する手段である。

次に、図１３を参照して本発明の第７の実施例に係る情報処理方法を説明する：

（ａ）まず、ステップＳ２０１において情報処理サーバ３０は、画像生成手段（モジュール）３２によって、第１通信端末２０ａから認証依頼を受信すると、ステップＳ２０２において、ワンタイムパスワードや日時などの情報を含む認証画像を生成し、認証パラメータ記憶装置１０１に記憶する。更にステップＳ２０３において、情報処理サーバ３０は、生成した認証画像を第１通信端末２０ａに送信する。

（ｂ）第１通信端末２０ａは、ステップＳ２０３において認証画像を受信すると、受信した画像をステップＳ２０４において提示する。

（ｃ）ステップＳ２０４において第１通信端末２０ａで認証画像が提示されると、ステップＳ２０５において第２通信端末（認証端末）２０ｂは提示された認証画像を撮影し、画像データ記憶装置１２ｂに記憶する。更にステップＳ２０６において第２通信端末（認証端末）２０ｂは、画像データ記憶装置１２ｂに記憶された認証画像の情報と、認証識別子記憶装置３０２ａに記憶された第２通信端末（認証端末）２０ｂの認証識別子を併せて認証情報を作成し、ステップＳ２０７において、認証情報を情報処理サーバ３００７に送信する。

（ｄ）ステップＳ２０７において、情報処理サーバ３

０は第２通信端末（認証端末）２０ｂから認証情報を受信すると、認証情報取得手段（モジュール）１１２によって、受信した認証情報を認証情報記憶装置１０２に記憶し、ステップＳ２０８において認証情報照合手段（モジュール）１１３によって認証パラメータ記憶装置１０１、認証情報記憶装置１０２、認証識別子記憶装置３０２ｂを参照して認証情報の照合を行う。

（ｅ）認証情報の認証結果が出ると、情報処理サーバ３０は、第１通信端末２０ａに認証結果を送信し、第１通信端末２０ａは認証結果取得手段（モジュール）２１３によって認証結果を受信する。

本発明の第７の実施例に係る情報処理サーバ３０によると、第２通信端末（認証端末）２０ｂの認証情報を利用することにより、認証情報を備えていない第１通信端末２０ａを認証することができる。したがって、ユーザは１つの第２通信端末（認証端末）２０ｂを備えていれば、複数の端末について同様に認証を受けることができる。

更に、本発明の第７の実施例によれば、本来は携帯電話機で入力しなければならない情報を、ユーザインターフェースの充実しているコンピュータで入力し、更に、セキュリティレベルの高い状態で、その入力した情報をサーバに送信することができる。

（第８の実施例）

図１４に示した本発明の第８の実施例に係る情報処理システムは、図１２に示した本発明の第７の実施例に係る情報処理システムに比べて、コンテンツ提供サーバ５を備えている点が異なる。更に、第１通信端末２０ａにおいて、認証結果取得手段（モジュール）２１３を備えておらず、コンテンツ取得手段（モジュール）２１４を備えている点が異なる。

本発明の第８の実施例に係る情報処理サーバ３０は、画像生成手段（モジュール）３２において、コンテンツ提供サーバ５から、第１通信端末２０ａの認証依頼を受信し、認証情報照合手段（モジュール）１１３において、結果をコンテンツ提供サーバ５に送信する。

本発明の第８の実施例に係るコンテンツ提供サーバ５は、情報処理サーバ３０及び第２通信端末（認証端末）２０ｂの情報を利用して第１通信端末２０ａを認証し、認証された第１通信端末２０ａにコンテンツを配信するものであって、コンテンツ記憶装置５０１、認証依頼手段（モジュール）５１１、認証結果取得手段（モジュール）５１２、コンテンツ配信手段（モジュール）５１３を備えている。

コンテンツ記憶装置５０１は、コンテンツ提供サーバ５が提供するコンテンツが記憶された記憶装置である。

認証依頼手段（モジュール）５１１は、例えば第１通

信端末２０ａからコンテンツの取得依頼があると、情報処理サーバ３０に対して、第１通信端末２０ａの認証を依頼する手段である。

認証結果取得手段（モジュール）５１２は、認証依頼手段（モジュール）５１１で依頼した第１通信端末２０ａの認証結果を、情報処理サーバ３０から取得する手段である。

コンテンツ配信手段（モジュール）５１３は、第１通信端末２０ａが認証されると、コンテンツ記憶装置５０１に記憶されたコンテンツを第１通信端末２０ａに送信する手段である。

図１４においては、本発明の第８の実施例に係るコンテンツ提供サーバ５は、第１通信ネットワーク７０ａに接続されているが、情報処理サーバ３０と相互に通信可能ならば、どの通信ネットワークに接続されても良い。

図１５を参照して、本発明の第８の実施例に係る情報処理方法を説明する：

（ａ）まず、ステップＳ３０２において、第１通信端末２０ａからコンテンツ提供サーバ５にコンテンツの要求がされると、コンテンツ提供サーバ５は、ステップＳ３０２において認証依頼手段（モジュール）５１１によって、情報処理サーバ３０に第１通信端末２０ａの認証を依頼する。

（ｂ）その後、ステップＳ３０３乃至ステップ２０９

の処理は、図１３のステップＳ２０２乃至ステップＳ２０８の処理と同様なので説明を割愛する。

（ｃ）ステップＳ３０９において、情報処理サーバ３０において認証結果が出ると、情報処理サーバ３０はステップＳ３１０において、第１通信端末２０ａの認証結果をコンテンツ提供サーバ５に送信する。

（ｄ）コンテンツ提供サーバ５は、認証が許可されると、ステップＳ３１１においてコンテンツ記憶装置５０１から第１通信端末２０ａにコンテンツを提供する。

この方法は、第１通信端末２０ａにおいて一般的なブラウザを利用してコンテンツ提供サーバ５からコンテンツを取得する場合に有効である。

次に、図１６を参照して、本発明の第８の実施例の変形例に係る情報処理方法について説明する。

（ａ）まず、ステップＳ３５１において、第１通信端末２０ａがコンテンツ提供サーバ５にコンテンツを要求すると、ステップＳ３５２において、コンテンツ提供サーバ５は、第１通信端末２０ａに認証情報を要求する。

（ｂ）これを受けて第１通信端末２０ａは、ステップＳ３５３において情報処理サーバ３０に認証依頼を行う。

（ｃ）その後、ステップＳ３５４乃至ステップ２６０の処理は、図１３のステップＳ２０２乃至ステップＳ２０８の処理と同様なので説明を割愛する。

（ｄ）ステップＳ３６０において、情報処理サーバ３

０において認証結果が出ると、情報処理サーバ３０はステップＳ３６１において、第１通信端末２０ａの認証結果を第１通信端末２０ａに送信し、これを受けて第１通信端末２０ａは、ステップＳ３６２において認証結果をコンテンツ提供サーバ５に送信する。

（ｅ）コンテンツ提供サーバ５は、認証結果を受信すると、認証が許可されている場合、ステップＳ３６３においてコンテンツ記憶装置５０１から第１通信端末２０ａにコンテンツを提供する。

この方法は、第１通信端末２０ａにおいて、コンテンツ提供サーバ５や情報処理サーバ３０が提供する認証依頼プログラムを含むアプリケーションによって、コンテンツ提供サーバ５にコンテンツを提供する場合に有効である。

本発明の第８の実施例によれば、情報処理サーバ３０は、複数のサーバの認証機能を受け付けることができ、様々なサーバに高いセキュリティレベルの認証を行わせることができる。

（第９の実施例）

本発明の第１及び第８の実施例においては、第１通信端末２０ａの認証について主に説明したが、本発明の第９の実施例においては、第１通信端末２０ａ及び第２通信端末（認証端末）２０ｂを操作するユーザの認証につ

いて説明する。

図１７に示す本発明の第９の実施例に係る情報処理サーバ３０は、図１２に示す本発明の第７の実施例に係る情報処理サーバ３０と比べて、リマインダー質疑応答記憶装置１０４、リマインダー質疑応答登録手段（モジュール）１１４、パスワード再発行手段（モジュール）１１５を備えている点が異なる。更に、第９の実施例に係る第２通信端末（認証端末）２０ｂは、第７の実施例に係る第２通信端末（認証端末）２０ｂに比べて、リマインダー質疑応答登録手段（モジュール）３１３、再発行パスワード取得手段（モジュール）３１４を備えている点が異なる。

リマインダー質疑応答登録手段（モジュール）１１４は、第２通信端末（認証端末）２０ｂのリマインダー質疑応答登録手段（モジュール）３１３によって複数ある質疑応答の内、ユーザにユーザが答えられる複数の質疑応答を選択させ、ユーザの認証識別子に関連づけて、そのユーザが選択した質疑応答とその答えをリマインダー質疑応答記憶装置１０４に記憶させる手段である。

パスワード再発行手段（モジュール）１１５は、ユーザがパスワードを忘れてしまった場合、第２通信端末（認証端末）２０ｂの再発行パスワード取得手段（モジュール）３１４によってパスワードの再発行が要求されると、リマインダー質疑応答記憶装置１０４を参照してユーザが選択した質問をユーザに答えさせ、リマインダー質疑

応答記憶装置１０４に記憶された応答と一致するかを判定し、全ての質疑に答えられた場合、ユーザにパスワードを発行する手段である。

図１８に示すように、本発明の第９の実施例の情報処理サーバ３０が提示する複数の質疑応答は、質疑の候補、応答のセレクトリストの項目を備えている。更に、質疑のジャンルとセレクトリストのセレクト数の項目を備えていても良い。ユーザはこれらの質疑の候補の中から、ユーザ自身が確実に答えられる質問を所定の数（例えば４つなど）以上を、ユーザに選択させる。この様にユーザが登録時に４問以上選択することになる場合、１１問から４問以上を選択する組合せの数は、１８１７通りとなる。

例えば、「お母さんは何日生まれ？」という質問がユーザに選択されたとすると、セレクトリストとしては１～３１日が挙げられ、ユーザはその中から正解を選択する。これらを所定の数だけ繰り返し、第２通信端末（認証端末）２０ｂは、情報処理サーバ３０に送信する。例えば、選択数１５の質疑をユーザが４つ選択したとすると、その回答の組合せは、１５の４乗となり、５０６２５通りにも及ぶ。この様な方法を取ることにより、ユーザの選択した質疑とその応答を解読するのは不可能になり、より高いセキュリティレベルを保つことができる。

例えば、図１９に示すように、英数字だけのパスワードによると、英数字（Ａ～Ｚまでの英字２６文字と０か

ら９までの数字１０個）を組合せると、３６文字の４乗で１，６７９，６１６通りあることを示す。

一方、本発明の第９の実施例で説明した方法によると、図１８に示す様に１１の質問から４つを選択し、その４つについて５０，６２５通りのセレクトリストの組合せがあるとすると、ユーザが取り得る組合せは、少なく見積もっても９１，９８５，６２５通り以上となる。これは、図１９を参照すると分かるように、英数字のみをパスワードにした場合、５～６桁の、数字のみをパスワードにした場合、７～８桁の強度があることが分かる。

図２０を参照して、本発明の第９の実施例に係る情報処理方法について説明する：

（ａ）まず、リマインダー質疑応答を登録する場合、ステップＳ４０１において情報処理サーバ３０は第２通信端末（認証端末）２０ｂに質問と、回答の選択肢の組合せを送信し、ユーザに確実に回答できる質問とその答えを決定させる。次に、ステップＳ４０２において、情報処理サーバ３０は第２通信端末（認証端末）２０ｂから、所定の数以上の質問と回答の組合せを受信し、リマインダー質疑応答記憶装置１０４に記憶する。

（ｂ）更にパスワードを再発行する場合、ステップＳ４５１において、情報処理サーバ３０は第２通信端末（認証端末）２０ｂからパスワードの再発行依頼を受信すると、ステップＳ４５２において、情報処理サーバ３０は

第２通信端末（認証端末）２０ｂに、ステップＳ４０１で送信した質問と回答の選択肢の組合せと同じものを送信し、ユーザにステップＳ４０２で回答した質問に回答させる。

（ｃ）更に、ステップＳ４５３において、第２通信端末（認証端末）２０ｂから登録時に回答した質問と回答の組合せを受信すると、ステップＳ４５４においてリマインダー質疑応答記憶装置１０４を参照して回答を照合し、照合の結果、選択した質問と、その質問の回答の全てが一致していた場合、ステップＳ４５３においてパスワードを再発行する。

本発明の第９の実施例に係る情報処理システムによれば、非常に高いセキュリティレベルでユーザを認証することができる。

（第１０の実施例）

本発明の第１０の実施例に係る情報処理サーバ３０ａは、図２１に示すように、通信端末識別子によって検索される対応情報を格納する識別子対応情報記憶装置３４と、通信端末から入力される情報を、対応情報に従って変換する情報変換手段（モジュール）３３とを備える。更に、通信端末から入力される情報から画像を作成する画像生成手段（モジュール）３２と、通信端末との情報

のやり取りを制御する入出力制御手段（モジュール）３１とを備える。

識別子対応情報記憶装置３４には、通信端末の機種等を認識するための識別子をしたがって、情報を送信する際にどのように変換すれば良いかを規定した対応情報が格納されている。

情報変換手段（モジュール）３３は、識別子対応情報記憶装置３４から対応情報を読み出し、該当の通信端末に送る情報を実際に変換する。画像生成手段（モジュール）３２は、通信端末内に画像作成機能がない場合に、情報を画像化して通信端末に送信する。

本発明の第１０の実施例に係る情報処理システムでは、例えば図２１に示すように、情報処理サーバ３０ａに、第１通信ネットワーク７０ａを介して第１通信端末２０ａが接続し、更に、第２通信ネットワーク７０ｂを介して第２通信端末２０ｂが接続している。更に複数の通信端末が複数の通信ネットワークを介して接続しても構わない。

第１通信端末２０ａ及び第２通信端末２０ｂは、情報を二次元コード化して紙面等に記載された画像を読み取るためのカメラやスキャナ等の画像取込手段（モジュール）１１ａ、２１を備える。更に読み取った画像情報を格納しておく画像データ記憶装置１２ａ、２２を備える。又、通信端末の機種等を認識させるための識別子情報を格納しておく識別子情報記憶装置を備える。そして、情

報処理サーバ３０ａと通信知るための情報送受信手段（モジュール）と、受信した画像等の情報を表示するための画像表示画面とを備える。

次に、図２２を参照しながら、通信の手順を説明すると以下のようになる：

（ａ）ステップＳ５００において、第１通信端末２０ａは、二次元コード化された画像を画像取込手段（モジュール）１１ａによって端末内に取り込み、第１通信端末２０ａ自体の情報と共に情報処理サーバ３０ａに送信する。

（ｂ）ステップＳ５０１において、情報処理サーバ３０ａは、第１通信端末２０ａから受信した情報を元に、二次元コード化した画像の情報を第１通信端末２０ａに返信する：

ステップＳ５０２において、第１通信端末２０ａは、情報処理サーバ３０ａから受信した画像を画像表示画面１５ａに表示する。

（ｃ）ステップＳ５０３において、つづいて、第２通信端末２０ｂは、第１通信端末２０ａの画像表示画面１５ａに表示された画像を、画像取込手段（モジュール）１１ｂによって端末内に取り込み、識別子情報記憶装置１３ｂに格納された識別子情報と共に情報処理サーバ３０ａに送信する。

（ｄ）ステップＳ５０４において、情報処理サーバ３

０ａは、第２通信端末２０ｂから受信した識別子を元に、識別子対応情報記憶装置３４を検索し、情報を変換するための対応情報を読み出す。そして、その対応情報に従って情報を変換し、第２通信端末２０ｂに返信する。

この手順のステップＳ５０４の情報変換によって、異機種間の二次元コード化の記述方式の差分を吸収できるため、第１通信端末２０ａと第２通信端末２０ｂが異機種でも、二次元コード化した画像を介して、必要な情報を正常に伝達することができる。

＜第１０の実施例の具体例１：電話番号交換＞

（ａ）ステップＳ５００で、電話帳登録処理命令情報を二次元コード化した画像を読み取り、第１通信端末２０ａ自体の情報として、電話番号やメールアドレスを情報処理サーバ３０ａに送信する。

（ｂ）ステップＳ５０１では、電話帳登録処理命令情報と第１通信端末２０ａの電話番号やメールアドレスを一体にして二次元コード化した画像が第１通信端末２０ａに返信される。

（ｃ）ステップＳ５０２、ステップＳ５０３では、第１通信端末２０ａの画像表示画面１５ａに表示された画像を第２通信端末２０ｂで取り込み、第２通信端末２０ｂの識別子と共に情報処理サーバ３０ａに送信する。

（ｄ）ステップＳ５０４で、情報処理サーバ３０ａで

受信した画像は、第２通信端末２０ｂが解釈できる情報に変換される。そしてその情報を受信した第２通信端末２０ｂでは、電話帳に第１通信端末２０ａの電話番号やメールアドレスが登録させる。

同じ手順で、第２通信端末２０ｂの電話番号やメールアドレスを、第１通信端末２０ａの電話帳に登録することで名刺交換と同様のことが二次元コード化画像を夜に込むことで可能になる。又、第２通信端末２０ｂが画像生成機能を備えている場合は、第１通信端末２０ａの機種情報を得ておけば、第２通信端末２０ｂ内で画像を生成して、第１通信端末２０ａに直接読込ませることで、情報を伝達することができる。

＜第１０の実施例の具体例２：複数端末情報＞

（ａ）ステップＳ５００で、相性占い処理命令情報を二次元コード化した画像を読み取り、第１通信端末２０ａ自体の情報として、生年月日や名前を情報処理サーバ３０ａに送信する。

（ｂ）ステップＳ５０１では、相性占い処理命令情報と第１通信端末２０ａの生年月日や名前を一体にした情報か途中の占い結果を二次元コード化した画像が、第１通信端末２０ａに返信される。

（ｃ）ステップＳ５０２、ステップＳ５０３では、第１通信端末２０ａの画像表示画面１５ａに表示された画

像を第２通信端末２０ｂで取り込み、第２通信端末２０ｂ´の情報として、識別子と生年月日や名前を共に情報処理サーバ３０ａに送信する。

（ｄ）ステップＳ５０４での情報変換では、第２通信端末２０ｂからの情報を元に相性占いプログラムを実行した結果を第２通信端末２０ｂに返信する。更に第１通信端末２０ａにも結果を返信しても良い。

（第１１の実施例）

本発明の第１１の実施例に係る情報処理サーバ３０ｂは、図２３に示すように、第１０の実施例に係る情報処理サーバ３０ａに、通信端末が情報交換を許可されているか示す許可情報を格納する許可情報記憶装置３６と、許可情報を判定する許可判定手段（モジュール）３５とを更に備えたものである。

許可情報記憶装置３６は、各端末の電話番号や端末番号等の識別情報で検索することで読み出すことができる、通信許可／不許可を規定している情報を格納している。そして許可判定手段（モジュール）３５は、その許可情報を読み出し、通信をしてよいかを判定し、許可なら処理を続行させ、不許可ならエラー処理を行う。

本発明の第１１の実施例に係る情報処理システムは、図２３に示すように、第１０の実施例に係る情報処理システムと同様である。

次に、図２４及び図２５を参照しながら、通信の手順を説明すると以下のようになる：

（ａ）ステップＳ６００からステップＳ６０３までは、図２２のステップＳ５００からステップＳ５０３までと同様である。

（ｂ）ステップＳ６０４において、情報処理サーバ３０ｂは、第２通信端末２０ｂの識別情報を元に許可情報記憶装置３６から許可情報を読み出す。その許可情報を許可判定手段（モジュール）３５によって判定する。

（ｃ）ステップＳ６０５において、もし情報の交換が許可されている場合、図２２のステップＳ５０４と同様に、情報処理サーバ３０ｂは、識別子対応情報記憶装置３４を検索し、情報を変換するための対応情報を読み出す。そして、その対応情報に従って情報を変換し、第２通信端末２０ｂに返信する。

（ｄ）ステップＳ６０６において、もし情報の交換が不許可の場合、エラー情報を第２通信端末２０ｂに返信する。

この手順により、情報を共有できる端末、できない端末とグループ化することができ、情報のセキュリティを高めることができる。又、アクセス時刻等の情報をキーとして許可情報を許可情報記憶装置３６に格納しておくことも可能である。これによって時間帯による規制等をかけることができる。

（第１２の実施例）

図２６は、インターネット（通信ネットワーク）７０に接続される携帯情報端末（第１端末）２０と、事業者サーバ（第２端末）５１と、情報処理サーバ３０とに着目した本発明の第１２の実施例に係る情報処理システムの構成図である。ここで、「携帯情報端末（第１端末）２０」とは、第１～第１１の実施例で説明したと同様な、カメラ、赤外線スキャナなど各種スキャナを含む種々の画像コード読取装置１９を備える携帯情報端末である。「画像コード」も、第１～第１１の実施例でと同様な、一次元コード、二次元コード、ホログラムコード、ウォータマーク（すかし技術）、ステガノグラフィー（画像への情報埋め込み）や、種々の他の自動認識コード等を含むものである。具体的には、「画像コード」の一例として、ＱＲコードと呼ばれるマトリクス型の二次元コードである情報コードと、情報コードの周囲を取り囲むように配置された識別力を有する情報コードとで構成しても良い。情報コードの一辺の長さは、例えば、８～１５ｍｍ（外側のマージン込みで１０～１８ｍｍ）程度にすることが可能である。ＱＲコードの他、情報コードとしては、国際標準規格になっているCode 16、Code 49、MaxiCode、Data Matrix、Code One等の二次元コード、或いはスキャントークコードを用いても良い。識別コードは、

例えば、情報コードの周囲の空白部分の長さを、セルの一辺の４倍の長さとすることができる。ここで、「セル」とは、情報コードの最小描画単位を指す。

現実には、インターネット（通信ネットワーク）７０には、複数の事業者サーバ（第２端末）５１と、複数の携帯情報端末（第１端末）２０が接続されうるが、説明を簡単にするために、単一の事業者サーバ（第２端末）５１と、単一の携帯情報端末（第１端末）２０を図示している。本発明の第１２の実施例に係る情報処理システムは、やり取りをしたい携帯情報端末（第１端末）２０と事業者サーバ（第２端末）５１が認証する際に、携帯情報端末（第１端末）２０と事業者サーバ（第２端末）５１の間に別の認証のための情報処理サーバ３０が仲介して認証を行う方式である。実際には、携帯情報端末（第１端末）２０は、デジタル通信網（他の通信ネットワーク）に接続され、このデジタル通信網が中継処理装置を介して、インターネット（通信ネットワーク）７０に接続される構成で構わない。デジタル通信網には複数の移動通信加入者交換機が接続され、この移動通信加入者交換機には複数の無線中継機が接続されるようなシステム構成等でも良い。即ち、携帯情報端末（第１端末）２０から発信された情報は、無線中継機を介し、移動通信加入者交換機に送信され、この移動通信加入者交換機からデジタル通信網を介して中継処理装置に情報が送信され、この中継処理装置が、通信ネットワーク７０とデジタル

通信網のデータの仲介を行うようなシステムを図２６は含み得ると理解すべきである。

図２６に示した情報処理サーバ３０は、アクション要求受信手段（モジュール）３２１と、事業者サーバ認証手段（モジュール）３２２と、個人・端末認証手段（モジュール）３２３と、整理券情報発行手段（モジュール）３２４と、整理券情報認証手段（モジュール）３２５と、個人情報送信許可手段（モジュール）３２６と、必要最小限情報送信手段（モジュール）３２７とを有するＣＰＵ３２０を備える。更に、このＣＰＵ３２０には、事業者情報登録装置３７と、個人情報登録装置３８と整理券情報記憶装置３９が接続されている。

ここで、アクション要求受信手段（モジュール）３２１は、携帯情報端末（第１端末）２０からのアクション要求の受信をする手段である。又、事業者サーバ認証手段（モジュール）３２２は、事業者サーバ（第２端末）５１の認証をする論理回路で、個人・端末認証手段（モジュール）３２３は、携帯情報端末（第１端末）２０の認証をする論理回路で、整理券情報発行手段（モジュール）３２４は、アクション要求を行った携帯情報端末（第１端末）２０に認証情報（整理券情報）を発行する論理回路で、整理券情報認証手段（モジュール）３２５は、認証情報（整理券情報）が正しいか判定する論理回路である。更に、個人情報送信許可手段（モジュール）３２

６は、個人情報の送信を許可する論理回路で、必要最小限情報送信手段（モジュール）３２７は、認証情報（整理券情報）に基づき、要求されたアクションに必要最小限の情報のみを事業者サーバ（第２端末）５１に送信する論理回路である。一方、事業者情報登録装置３７は事業者情報を記憶する記憶装置である。又、個人情報登録装置３８は、認証対象となる個人情報記憶する記憶装置である。整理券情報記憶装置３９は、発行する認証情報（整理券情報）を記憶する記憶装置である。

一方、携帯情報端末（第１端末）２０は、上記の画像コード読取装置１９に加え、処理制御装置２１、画像表示装置１５、画像データ記憶装置１２及び個人情報記憶装置１８等を備える。処理制御装置２１は、画像取込手段（モジュール）１１と、画像コード解読手段（モジュール）１３と、画像コード変換手段（モジュール）１４と、統合データ編集手段（モジュール）１６と、電話機能制御手段（モジュール）１７とを有する。この処理制御装置２１には、画像コード読取装置１９と、画像表示装置１５と、画像データ記憶装置１２と、個人情報記憶装置１８とが接続されている。

処理制御装置２１の画像コード解読手段（モジュール）１３は、画像コード読取装置１９で読込まれたデータを取得し、２次元コード等の画像コードが正当であるかどうかのチェックを行う。画像コード変換手段（モジュール）１４は、画像コード解読手段（モジュール）１３で

読込まれた画像コードを文字データに変換する。画像コード解読手段（モジュール）１３及び画像コード変換手段（モジュール）１４を経ることによって、画像コードは、単なる画像データからコンピュータ読み取り可能なデータに変換することができる。統合データ編集手段（モジュール）１６は、個人情報記憶装置１８に記憶された個人情報と、画像コード変換手段（モジュール）１４より得られた商品情報を編集統合し、外部に発信する手段（モジュール）である。画像コード読取装置１９は、広告媒体に書かれた商品掲載ページ、商品情報などの商品に関する情報が埋め込まれた画像コードを読み取り、本発明の第１２の実施例に係る携帯情報端末（第１端末）２０に取り込むものである。

個人情報記憶装置１８は、所有者（ユーザ）の個人情報を「第１レベルの個人情報」と「第２レベルの個人情報」とに分けて記憶する。「第１レベルの個人情報」とはユーザの氏名や登録番号等の携帯情報端末（第１端末）２０の認証に必要な最低限の情報で、セキュリティレベルの低い個人情報である。「第２レベルの個人情報」とは第１レベルの個人情報よりもセキュリティレベルの高く、重要な個人情報で、例えば、住所、電子メールアドレス、クレジットカード番号、銀行口座名、給与、資産、家族構成の情報、身体的特徴等が含まれうる。一時記憶装置は、画像コード読取装置１９から読み取られたコードや、画像コード解読手段（モジュール）１３及び画像

コード変換手段（モジュール）１４で得られるコードを一時保存するための記憶装置である。図２６には特に表示していないが、入力装置、無線装置、音声処理装置、ＣＯＤＥＣ（コーデック）、データ記憶装置、一時記憶装置、及びこれらの各装置が正常に機能するための電源回路や電池（バッテリー）等が備えられていることは勿論である。

図２７のフローチャートを用いて、本発明の第１２の実施例に係る情報処理方法を説明する：

（ａ）まず、ステップＳ７０１において、携帯情報端末（第１端末）２０は、紙媒体等に印刷された画像コードを読み取り、個人情報記憶装置１８に記憶された第１レベルの個人情報と、画像コードに含まれる商品情報を編集統合した統合情報を、アクション要求を仲介するサーバである情報処理サーバ３０に送信する。そして、ステップＳ７０２において、情報処理サーバ３０は携帯情報端末（第１端末）２０からのアクション要求の受信をする。

（ｂ）その後、ステップＳ７０３において、情報処理サーバ３０は、事業者情報登録装置３７及び個人情報登録装置３８に記録された内容を参照して、事業者サーバ（第２端末）５１の認証及び携帯情報端末（第１端末）２０の認証をする。

（ｃ）ステップＳ７０３において、事業者サーバ（第

２端末）５１の認証と携帯情報端末（第１端末）２０の認証ができたら、ステップＳ７０４において、情報処理サーバ３０はアクション要求を行った携帯情報端末（第１端末）２０に認証情報（整理券情報）を発行する。更に、発行した認証情報（整理券情報）を整理券情報記憶装置３９に記憶する。

（ｄ）即ち、安全を確認できれば、携帯情報端末（第１端末）２０からの第２レベルの個人情報の送信が許可される。すると、ステップＳ７０５において、携帯情報端末（第１端末）２０は、情報処理サーバ３０に対し、この第２レベルの個人情報を認証情報（整理券情報）と共に送信する。第２レベルの個人情報は、個人情報記憶装置１８に記憶されているものの他、携帯情報端末（第１端末）２０の入力装置を用いて、新たに入力された必要最小限の情報でも良い。

（ｅ）次に、情報処理サーバ３０は、第２レベルの個人情報と認証情報（整理券情報）とを受信する。そして、ステップＳ７０６において、受信した認証情報（整理券情報）に基づき、要求されたアクションに必要最小限の情報（第２レベルの個人情報）のみを事業者サーバ（第２端末）５１に送る。

図２７に示す第１２の実施例に係る情報処理方法によれば、不必要なデータを送信せず、かつお互いの不必要な情報を入手しなくても携帯情報端末（第１端末）２０と事業者サーバ（第２端末）５１間の認証を可能とする。

図２８は、第１２の実施例に係る情報処理方法の実施に用いる情報処理サーバ３０の動作を説明するフローチャートである。

（ａ）まず、ステップＳ７１１において、情報処理サーバ３０のアクション要求受信手段（モジュール）３２１は、携帯情報端末（第１端末）２０からのアクション要求の受信を第１レベルの個人情報とともにする。そして、ステップＳ７１２において、事業者サーバ認証手段（モジュール）３２２は事業者サーバ（第２端末）５１の認証をする。更に、ステップＳ７１３において、個人・端末認証手段（モジュール）３２３が携帯情報端末（第１端末）２０の認証をする。

（ｂ）ステップＳ７１２における事業者サーバ（第２端末）５１の認証、及びステップＳ７１３における携帯情報端末（第１端末）２０の認証が完了したら、ステップＳ７１４において、情報処理サーバ３０の整理券情報発行手段（モジュール）３２４は、アクション要求を行った携帯情報端末（第１端末）２０に認証情報（整理券情報）を発行する。

（ｃ）ステップＳ７１５において、情報処理サーバ３０の整理券情報認証手段（モジュール）３２５は、認証情報（整理券情報）が正しいか判定し、正しければ、ステップＳ７１６において、個人情報送信許可手段（モジュール）３２６は、第２レベルの個人情報の送信を携帯

情報端末（第１端末）２０に許可する。

（ｄ）情報処理サーバ３０は、この第２レベルの個人情報を認証情報（整理券情報）と共に受信する。そして、ステップＳ７１７において、情報処理サーバ３０の必要最小限情報送信手段（モジュール）３２７は、認証情報（整理券情報）に基づき、携帯情報端末（第１端末）２０から要求されたアクションに必要最小限の情報（第２レベルの個人情報）のみを事業者サーバ（第２端末）５１に送信する。

第１２の実施例に係る情報処理システムは、携帯情報端末２０に「エンクリプティッド・ランダムナンバー・メタデータベースシステム」を採用しても良い。「エンクリプティッド・ランダムナンバー・メタデータベースシステム」とは、携帯情報端末２０の個人情報記憶装置１８に「第１レベルの個人情報」の代わりに固有の無限に長い乱数の組を保持し、動的に発行するセッションＩＤと組み合わせ、情報処理サーバ３０でこの識別情報を個人情報に変換する方式である。

図２７のフローチャートにおけるステップＳ７０３又は図２８のフローチャートにおけるステップＳ７１２でアクションを要求する際、個人・端末認証のため、携帯情報端末２０から、携帯情報端末２０固有の情報や個人認証のための第１レベルの個人情報を受信する必要がある。エンクリプティッド・ランダムナンバー・メタデー

タベースシステムを用いることにより、携帯情報端末２０から最初に発信される第１レベルの個人情報は乱数であるため、安全に、より情報が第３者に不当に漏れないシステムとなる。

図２６に示した第１２の実施例に係る情報処理システムにおいて、情報処理サーバ３０を、第１の実施例に係る個人情報保護方式のメタサーバ７６と同様に、各処理毎に分割し、複数のサーバ７２，７３，７４として実装し、通信ネットワーク７０上に出回るデータはそのデータを処理するサーバのみで復号できる形で暗号化することによって、分割されたサーバでは処理に必要なデータ以外は復号化できないようにすることができる（図１参照。）。

即ち、図２６に示す情報処理サーバ３０を、図１に示すメタサーバ７６に対応して、複数のサーバ７２，７３，７４，・・・・・で構成する。そして、図２７のフローチャートのステップＳ７０５においては、第１端末２０内において、複数のサーバ７２，７３，７４，・・・・・の数に対応した複数の情報を、複数のサーバ７２，７３，７４，・・・・に１：１にそれぞれ対応した複数の暗号化鍵でそれぞれ暗号化して、複数のサーバ７２，７３，７４，・・・・・の数に対応した複数の暗号化情報E_1，E_2，E_3，・・・・・，E_nを生成する。そして、情報処理サーバ（メタサーバ）３０が、複数の暗号化情報E_1，E_2，E_3，・・・・・，E_nを受信し、複数のサーバ７２，７３，７４，・・・・・のそれぞ

れで、複数の暗号化情報E_1, E_2, E_3, ・・・・・, E_nを順次復号する。

即ち、第１の情報をメタサーバ内の第１サーバ７２用の暗号化鍵で暗号化して第１の暗号化情報E_1を生成し、第２の情報をメタサーバ内の第２サーバ７３用の暗号化鍵で暗号化して第２の暗号化情報E_2を生成し、第３の情報をメタサーバ内の第３サーバ７４用の暗号化鍵で暗号化して第３の暗号化情報E_3を生成し、・・・・・、第ｎの情報をメタサーバ内の第ｎサーバ用の暗号化鍵で暗号化して第ｎの暗号化情報E_nを生成し、第２レベルの個人情報を生成する。

そして、第１の暗号化情報E_1、第２の暗号化情報E_2、第３の暗号化情報E_3、・・・・・、第ｎの暗号化情報E_nをメタサーバ（情報処理サーバ）３０が第２レベルの個人情報として受信する。その後、メタサーバ（情報処理サーバ）３０の第１サーバ７２で、第１の暗号化情報E_1を復号して処理し、第２サーバ７３で、第２の暗号化情報E_2を復号して処理し、第３サーバ７４で、第３の暗号化情報E_3を復号して処理し、・・・・・、第ｎサーバで、第ｎの暗号化情報E_nを復号する。そして、図２７のフローチャートのステップＳ７０６、若しくは図２８のステップＳ７１７において、第２レベルの個人情報を事業者サーバ（第２端末）５１に送る。

或いは、第１の実施例に係る個人情報保護方式において、図１、図２及び図３を参照して説明したように、暗

号化された情報を検索キーとし、その暗号化された検索キー情報から関連づけられる暗号データを検索することが可能なように、暗号化データベースを実現しても良い。

第１２の実施例に係る情報処理システムにおいて、情報処理サーバ３０にアクションを行う事業者サーバへ送信するための情報を受け渡す際に、第１の実施例及び第１の実施例に係る個人情報保護方式を用いることにより、情報処理サーバ３０では、他のサーバと結託しキーを入手しない限り、その情報の中身を見ることが不可能であり、情報処理サーバ３０で誰が何をしようとしたのか知ることはできない。つまり、内部のサーバ管理者でさえ情報が漏れない仕組みとなる。

更に、情報処理サーバ３０側に第１の実施例に係る個人情報保護方式を採用し、携帯情報端末２０に「エンクリプティッド・ランダムナンバー・メタデータベースシステム」を採用することにより、情報が外部からの攻撃だけでなく、内部の人でさえ、不当に漏れない認証代行モデルとなる。

更に、情報処理サーバ３０側に第２～６の実施例に係る種々の個人情報保護方式を採用することにより、情報が外部からの攻撃だけでなく、内部の人でさえ、不当に漏れない認証代行モデルが実現できる。

＜第１２の実施例の第１変形例：チケットシステム＞

イベント会場への第１２の実施例の応用を考えてみる。

まず、図２７のフローチャートに示したように、携帯情報端末２０を利用し、ステップＳ７０１において紙誌面、パーソナルコンピュータ、ＷＥＢサイトなどから、興行（日時、座席、会場など）の選択し、その画像コードを撮り、情報処理サーバ３０に送信する。そして、ステップＳ７０２及びステップＳ７０３を経て、ステップＳ７０４において、情報処理サーバ３０が携帯情報端末２０に整理券情報を発行する。その後、ステップＳ７０５及びステップＳ７０６を経て、チケットの予約・決済がされる。そして、イベント会場入り口では、入場管理者が、携帯情報端末２０のチケット認証画像コードを読み、サーバで支払い証明を確認し、支払済みであれば、「特定の画像」（ＯＫなど）を表示し、管理者が視認し、入場させる。しかしながら、イベント会場入り口での「入場」の操作において時間がかかると、入場が混雑することが考えられる。又、混雑を回避するために、前もってチケット認証画像コード読ませると、前もって読んで特定の画像を得たユーザが他のユーザに携帯経由で転送することが可能なため、入場における認証として役割を果たさない。

この問題点を解決するため、第１２の実施例の変形例に係るチケットシステムは、図２９のフローチャートに示す方法を採用する：

（ａ）まず、ステップＳ７６１において、チケット認証カードを印刷した印刷物を複数個用意する。「印刷物」

は、適当な大きさのカードのようなもので良く、画像コードの下に、固有番号が視認可能な形で印刷されている。例えば、２Ａ８４ＲＴ４などの固有番号が、画像コードの下に印刷されている。この画像コードは、例えば、ＱＲコードと呼ばれるマトリクス型の二次元コードと、この二次元コードの周囲を取り囲む情報コードとで構成しても良い。以下において、画像コードと番号をセットで印刷したカードを「チケット認証カード」と呼ぶ。なお、画像コードの下に印刷されている固有番号は、認証画像コード内にも埋め込まれている。

（ｂ）そして、ステップＳ７６２において、チケット認証カードに含まれる画像コードを携帯情報端末２０で撮影する。更に、ステップＳ７６３において、携帯情報端末２０から画像コードの情報と第１レベルの個人情報の統合情報を情報処理サーバ３０に送信する。

（ｃ）このため、ステップＳ７６４において、情報処理サーバ３０は携帯情報端末２０からのアクション要求を受ける。次に、ステップＳ７６５において、情報処理サーバ３０は事業者サーバ５１の認証と、個人・端末認証をする。ステップＳ７６５において、事業者サーバ５１の認証と携帯情報端末２０の認証ができたら、情報処理サーバ３０は携帯情報端末２０に整理券情報を発行する。

（ｄ）携帯情報端末２０は、整理券情報を受信するとステップＳ７６６において、チケット認証カードに含ま

れる画像コードの情報と第２レベルの個人情報の統合情報を事業者サーバ５１に送信する。ステップＳ７６７では、事業者サーバ５１において、携帯情報端末２０の予約、支払の確認をする。

（ｅ）ステップＳ７６８において、事業者サーバ５１が、その固有番号を携帯情報端末２０に送信する。

（ｆ）イベント会場入り口では、入場管理者は、ステップＳ７６９において、携帯情報端末２０に表示された固有番号と、チケット認証カードに印刷された視認番号が一致していることを確認する。これは、「チケットを切る」のと同程度の時間で処理可能である。又、チケット認証カードは、印刷ベースで何枚でも発行可能である。又回収後、使いまわすことができる。

以上のように、第１２の実施例の変形例に係るチケットシステムによれば、専用読取装置なしで、電子チケットの発行が可能となり、チケットを切るのと同程度の時間（視認のみ）で、入場管理が可能である。

＜第１２の実施例の第２変形例：口座ロック決済＞

第１２の実施例に係る情報処理方法は、印刷物やパーソナルコンピュータ画面上にある画像コードを撮影するだけで、買い物から、代金の支払、つまり決済までを行うシステムの実現に応用できる特徴を有する。金融機関の決済における認証は、大きくは、図３０に示したプロセスから実現される。

（ａ）ステップＳ８０１において、携帯情報端末２０は、画像コードを読んで情報処理サーバ３０に決済を要求する。

（ｂ）情報処理サーバ３０は携帯情報端末２０からの決済の要求を受けると、ステップＳ８０２において、事業者サーバ５１の認証と、個人・端末認証をし、認証ができたら、携帯情報端末２０に整理券情報を発行する。

（ｃ）整理券情報を受けた携帯情報端末２０は、ステップＳ８０３において、再度、情報処理サーバ３０に決済を要求する。

（ｄ）そして、情報処理サーバ３０は、ステップＳ８０４において、事業者サーバ（金融機関）５１に決済を要求する。事業者サーバ（金融機関）５１は、携帯情報端末２０のユーザの対応口座の残金を確認し、ステップＳ８０５において携帯情報端末２０に決済の承認をする。

（ｅ）決済の承認がされれば、携帯情報端末２０のユーザは、対応口座から所望の金額の引き落としをする。

しかしながら、図３０に示したプロセスでは、ステップＳ８０４～ステップＳ８０５の操作の間にタイムラグが発生し、ステップＳ８０５がステップＳ８０７の後になれば、そのタイムラグの間に、ステップＳ８０７の他の事業者５２が対応口座から残金を先に引き落とす。こうなれば、ステップＳ８０５の引き落としが不可能になる可能性がある。

この問題点を解決するため、第１２の実施例の第２変

形例では、図３１に示すように、ステップＳ８１４において、口座ロック整理券を発行する。即ち、ステップＳ８１４において、情報処理サーバ３０から事業者サーバ（金融機関）５１に対して口座ロック整理券を発行して、口座ロック整理券に対応する携帯情報端末２０の操作が終了するまで、その口座をロックする方式である。

図３１を用いて、本発明の第１２の実施例の第２変形例に係る金融機関決済方法を説明する：

（ａ）ステップＳ８１１～Ｓ８１３までは、図３０のステップＳ８０１～Ｓ８０３と同様である。ステップＳ８１４の残金確認時に、情報処理サーバ３０から、事業者サーバ（金融機関）５１に対して口座ロック整理券を発行する。

（ｂ）口座ロック整理券を発行されると、事業者サーバ（金融機関）５１は、携帯情報端末２０のユーザからの引き落としまでの間、事業者サーバ（金融機関）５１の対応口座から引き落としが行われないよう対応口座をロックする。

（ｃ）そして、パスポート（口座ロック整理券）に対応するＩＤを持つユーザからの決済が行われたら、事業者サーバ（金融機関）５１の口座を開放する。

＜第１２の実施例の第３変形例：デポジット方式決済＞

図３０に示したように、ステップＳ８０４～ステップＳ８０５の操作の間にタイムラグが発生し、そのタイム

ラグの間に、他の事業者５２が対応口座から残金を先に引き落とすことにより、ステップＳ８０５の引き落としが不可能になることを防止するためには、図３２に示すように、これは、情報処理サーバ３０による決済のための一定額をとっておき、そこから引き落とすことにより、他の事業者５２から起こったステップＳ８２７～Ｓ８２８の操作に影響させないにできる：

（ａ）ステップＳ８２１～Ｓ８２３までは、図３０のステップＳ８０１～Ｓ８０３と同様である。しかし、１５の実施例の第３変形例に係るデポジット方式では、あらかじめ事業者サーバ（金融機関）５１の対応口座から、一定額を引き出しデポジットしておく。デポジットは、情報処理サーバ３０によるサービスに一意に対応しており、同時に複数の決済行為、割り込みが発生することはないように設定されている。

（ｂ）このため、情報処理サーバ３０は、ステップＳ８２４において、事業者サーバ（金融機関）５１に決済を要求すると、事業者サーバ（金融機関）５１は、携帯情報端末２０のユーザの対応口座の専用デポジットの方の残金を確認し、ステップＳ８２５において携帯情報端末２０に決済の承認をする。

（ｃ）決済の承認がされれば、携帯情報端末２０のユーザは、対応口座の専用デポジットから所望の金額の引き落としをする。

（第１３の実施例）

図３３は、インターネット（通信ネットワーク）７０に接続される一般通信端末（主第１端末）２０ｎ、カメラ付き携帯情報端末（補助第１端末）２０ｍ、事業者サーバ（第２端末）５１及び情報処理サーバ３０に着目した本発明の第１３の実施例に係る情報処理システムの構成図である。

ここで、カメラ付き携帯情報端末（補助第１端末）２０ｍとは、第１２の実施例に係る情報処理システムで説明したと同様な、画像コード読取装置１９を備えた携帯情報端末である。画像コード読取装置１９には、カメラ、赤外線スキャナなど各種スキャナ等が含まれる。「画像コード」には、第１～第１２の実施例と同様に、一次元コード、二次元コード、ウォータマーク（すかし技術）、ステガノグラフィー（画像への情報埋め込み）や、種々の他の自動認識コード等が含まれうる。図３３に示すように、カメラ付き携帯情報端末（補助第１端末）２０ｍは、画像コード読取装置１９の他、処理制御装置２１、画像表示装置１５、画像データ記憶装置１２、個人情報記憶装置１８とを備えている。そして、処理制御装置２１は、画像取込手段（モジュール）１１と、画像コード解読手段（モジュール）１３と、画像コード変換手段（モジュール）１４と、統合データ編集手段（モジュール）１６と、電話機能制御手段（モジュール）１７とを有す

る処理制御装置２１を備えている。一方、一般通信端末（主第１端末）２０ｎは、画像コード読取装置１９を備えないパーソナルコンピュータ等の通信端末を意味する。

現実には、インターネット（通信ネットワーク）７０には、複数の事業者サーバ（第２端末）５１、複数のカメラ付き携帯情報端末（補助第１端末）２０ｍ、複数の一般通信端末（主第１端末）２０ｎが接続されうるが、説明を簡単にするために、単一の事業者サーバ（第２端末）５１と、単一のカメラ付き携帯情報端末（補助第１端末）２０ｍ及び単一の一般通信端末（主第１端末）２０ｎを図示している。実際には、カメラ付き携帯情報端末（補助第１端末）２０ｍは、デジタル通信網（他の通信ネットワーク）に接続され、このデジタル通信網が中継処理装置を介して、インターネット（通信ネットワーク）７０に接続される構成で構わない。

図３３に示した情報処理サーバ３０は、画像コード画面送信手段（モジュール）３３１と、統合情報受信手段（モジュール）３３２と、携帯情報端末認証手段（モジュール）３３３と、要求画面送信手段（モジュール）３３４と、アクション実行手段（モジュール）３３５を有するＣＰＵ３２０を備える。更に、このＣＰＵ３２０には、事業者情報登録装置３７と個人情報登録装置３８が接続されている。

ここで、画像コード画面送信手段（モジュール）３３

１は、画像コードを含む画面の送信をする論理回路である。「画像コード」の内容には、一意に特定できる乱数（ワンタイムパスワードのようなもの）とタイムスタンプが格納されている。又、統合情報受信手段（モジュール）３３２は、カメラ付き携帯情報端末（補助第１端末）２０ｍからの、画像コードの内容と個人情報との統合情報の受信をする論理回路で、携帯情報端末認証手段（モジュール）３３３は、カメラ付き携帯情報端末（補助第１端末）２０ｍの認証をする論理回路で、要求画面送信手段（モジュール）３３４は、カメラ付き携帯情報端末（補助第１端末）２０ｍに要求された画面を送信する論理回路で、アクション実行手段（モジュール）３３５は、カメラ付き携帯情報端末（補助第１端末）２０ｍに対しアクションの実行をする論理回路である。

更に、第１２の実施例に係る情報処理システムと同様に、事業者情報登録装置３７は、事業者情報を記憶する記憶装置で、個人情報登録装置３８は、認証対象となる個人情報記憶する記憶装置である。

図３４のフローチャートを用いて、本発明の第１３の実施例に係る情報処理方法を説明する：

（ａ）まず、ステップＳ７２１で、一般通信端末（主第１端末）２０ｎの画面を見ているユーザは、画面上のインターフェースとして用意されている「画像コードの表示」ボタンをクリックし、情報処理サーバ３０に画像

コードの表示を要求する。

（ｂ）すると、情報処理サーバ３０は、ステップＳ７２２において、画像コードを含む画面を一般通信端末（主第１端末）２０ｎに送信する。そして、ステップＳ７２３において、ユーザは、一般通信端末（主第１端末）２０ｎの画面に表示された画像コードをカメラ付き携帯情報端末（補助第１端末）２０ｍで読み取る。これによりカメラ付き携帯情報端末（補助第１端末）２０ｍの統合データ編集手段（モジュール）１６は、一般通信端末（主第１端末）２０ｎの画面に表示された画像コードの内容（乱数＋タイムスタンプ）とカメラ付き携帯情報端末（補助第１端末）２０ｍ内の情報（個人認証ＩＤ（固定乱数））を統合した情報を編集し、統合情報を作成する。そして、カメラ付き携帯情報端末（補助第１端末）２０ｍは、統合データ編集手段（モジュール）１６が編集した統合情報を、情報処理サーバ３０に送信する。

（ｃ）ステップＳ７２４において、情報処理サーバ３０は、受信した統合情報と個人情報登録装置３８に格納されている情報を対照し、ユーザの認証を行う。但し、ステップＳ７２２においてタイムスタンプ情報を送付した時刻から時間があまりにも経っているものステップＳ７２４では認証しない。

（ｄ）ステップＳ７２４においてユーザの認証できれば、ステップＳ７２５において情報処理サーバ３０は、ユーザが求める画面を一般通信端末（主第１端末）２０

ｎに送信し、一般通信端末（主第１端末）２０ｎの画面に表示する。或いは、テップＳ７２５において情報処理サーバ３０は、ユーザが求めるアクションの実行をする。ステップＳ７２３、ステップＳ７２４が完了して認証しない限り、ステップＳ７２５に遷移しない。

図３５は、第１３の実施例に係る情報処理方法の実施に用いる情報処理サーバ３０の動作を説明するフローチャートである。

（ａ）一般通信端末（主第１端末）２０ｎから、情報処理サーバ３０に画像コードの表示の要求があると、情報処理サーバ３０の画像コード画面送信手段（モジュール）３３１は、ステップＳ７３１において、画像コードを含む画面を一般通信端末（主第１端末）２０ｎに送信する。

（ｂ）情報処理サーバ３０の統合情報受信手段（モジュール）３３２は、ステップＳ７３２において、カメラ付き携帯情報端末（補助第１端末）２０ｍからの、画像コードの内容と個人情報との統合情報の受信をする。

（ｃ）情報処理サーバ３０の携帯情報端末認証手段（モジュール）３３３は、ステップＳ７３３において、受信した統合情報と個人情報登録装置３８に格納されている情報を対照し、カメラ付き携帯情報端末（補助第１端末）２０ｍの認証をする。

（ｄ）ステップＳ７３３においてユーザの認証できれ

ば、情報処理サーバ３０の要求画面送信手段（モジュール）３３４は、ステップＳ７３４において、カメラ付き携帯情報端末（補助第１端末）２０ｍに要求された画面を送信する。又は、情報処理サーバ３０のアクション実行手段（モジュール）３３５は、ステップＳ７３４において、カメラ付き携帯情報端末（補助第１端末）２０ｍから要求されたアクションの実行をする。ステップＳ７３３においてユーザの認証できなければ、処理を終了する。

図３３には、インターネット（通信ネットワーク）７０に、事業者サーバ５１、情報処理サーバ３０、カメラ付き携帯情報端末２０ｍ及び一般通信端末２０ｎが接続された情報処理システムの構成図を示した。この場合、一般通信端末２０ｎを事業者が提供するサービス専用の端末（以下、「サービス専用端末２０ｎ」と言う。）とすれば、このサービス専用端末２０ｎを介するサービスにも適用できる。サービス専用端末２０ｎとして好適な例としては、コンビニに設置された端末などがある。サービス専用端末２０ｎにおけるサービスがユーザの住所や名前などは必要な場合、図３４及び図３５のフローチャートと同様な手順で、ユーザの認証をすることにより、そのユーザの情報を安全に獲得できる。更に、ユーザはそのサービス専用端末２０ｎに個人情報を入力する手間が省け、サービス専用端末２０ｎに表示された画像コー

ドを読むだけで済む。

又、第１３の実施例に係る情報処理方法と第１～第６の実施例で説明した個人情報保護方式とを組み合わせることが可能である。

又、第１３の実施例に係る情報処理方法において、パーソナルコンピュータなどの一般通信端末２０ｎのディスプレイ上に、メニュー・表などの形式でアイテムを表示しておき、或いは検索結果を表示し、それらに画像コード生成のリンクを貼っておくようにしても良い。この様にしておけば、その検索結果をダイナミックに光学読み取り可能な形式で画像コード化して表示するができる。の一般通信端末２０ｎのディスプレイ上に表示されるそれらの画像コードは、偽造改竄が不能である。この様な構成にしておけば、発行事業者が認証可能で、画像コードは、携帯情報端末２０で読み取り可能で、携帯情報端末２０によって、個人認証が可能となる（会員認証、決済系の認証が可能である。）。そして、携帯情報端末２０の個人情報記憶装置に格納された個人認証識別情報から、それに連結されているサーバなどから、個人情報を紐付けして取り出すことができない（名寄せできない。）という利点を有する。

この様に、第１３の実施例に係る情報処理方法によれば、全てのトランザクション、決裁・決済行為が、検索機能、選択機能、編集統合機能と連動することにより、ダイナミックに可能となる。例えば、インテリアを、テ

ーブルと椅子とライトを選択した場合、それらのセットを統合し、コード生成すれば、一発で発注完了することがある。

つまり、第１３の実施例に係る情報処理方法によれば、あらゆる通販・物販で選択済みのアイテムを一括発注できる。又、第１３の実施例に係る情報処理方法によれば、必要なセキュリティレベルに応じた長さのワンタイムパスワードなどをコード生成時に埋め込めばセキュリティ精度が任意にコントロールできる。

（第１４の実施例）

第１４の実施例に係る情報処理方法は、第１携帯情報端末２０ｐ及び第２携帯情報端末２０ｑ間のデータのやり取りにおける認証代行方式である。これは、異種機種である第１携帯情報端末２０ｐと第２携帯情報端末２０ｑ間のデータ処理を行う際にメタサーバ（情報処理サーバ）３０を介することにより異種機種間の記述方式の違いを回避して，データの処理を安全に可能とする方式である。

図３６は、インターネット（通信ネットワーク）７０に接続される事業者サーバ５１、情報処理サーバ３０、第１携帯情報端末２０ｐ及び第２携帯情報端末２０ｑに着目した、本発明の第１４の実施例に係る情報処理システムの構成図である。ここで、第１携帯情報端末２０ｐ

及び第２携帯情報端末２０ｑは、それぞれ第１２の実施例に係る情報処理システムで説明したと同様な、画像コード読取装置１９ｐ及び１９ｑを備えた携帯情報端末である。画像コード読取装置１９ｐ及び１９ｑには、既に説明したように、カメラ、赤外線スキャナなど各種スキャナが含まれうる。「画像コード」も、第１～第１３の実施例での説明と同様な、一次元コード、二次元コード、ホログラムコード、ウォータマーク（すかし技術）、ステガノグラフィー（画像への情報埋め込み）や、種々の他の自動認識コード等を含み得るものである。

図３６に示すように、第１携帯情報端末２０ｐは、画像コード読取装置１９ｐの他、処理制御装置２１ｐ、画像表示装置１５ｐ、画像データ記憶装置１２ｐ、個人情報記憶装置１８ｐとを備えている。そして、処理制御装置２１ｐは、画像取込手段（モジュール）１１ｐと、画像コード解読手段（モジュール）１３ｐと、画像コード変換手段（モジュール）１４ｐと、統合データ編集手段（モジュール）１６ｐと、電話機能制御手段（モジュール）１７ｐとを有する処理制御装置２１ｐを備えている。

一方、第２携帯情報端末２０ｑは、画像コード読取装置１９ｑの他、処理制御装置２１ｑ、画像表示装置１５ｑ、画像データ記憶装置１２ｑ、個人情報記憶装置１８ｑとを備えている。そして、処理制御装置２１ｑは、画像取込手段（モジュール）１１ｑと、画像コード解読手段（モジュール）１３ｑと、画像コード変換手段（モジ

ュール）１４ｑと、統合データ編集手段（モジュール）１６ｑと、電話機能制御手段（モジュール）１７ｑとを有する処理制御装置２１ｑを備えている。現実には、インターネット（通信ネットワーク）７０には、複数の事業者サーバ５１、複数の携帯情報端末２０ｐ，２０ｑ，・・・・が接続されうるが、説明を簡単にするために、単一の事業者サーバ５１と、第１携帯情報端末２０ｐ及び携帯情報端末２０ｑを図示している。実際には、第１携帯情報端末２０ｐ及び第２携帯情報端末２０ｑは、それぞれ、デジタル通信網（他の通信ネットワーク）に接続され、このデジタル通信網が中継処理装置を介して、インターネット（通信ネットワーク）７０に接続される構成で構わない。

図３６に示した情報処理サーバ３０は、第１携帯情報端末情報獲得手段（モジュール）３４１と、認証用画像コード生成手段（モジュール）３４２と、画像データ送信手段（モジュール）３４３と、第２携帯情報端末情報獲得手段（モジュール）３４４と、情報編集手段（モジュール）３４５と、編集情報送信手段（モジュール）３４６とを備える。

更に、このＣＰＵ３２０には、事業者情報登録装置３７と個人情報登録装置３８が接続されている。

ここで、第１携帯情報端末情報獲得手段（モジュール）３４１は、第１携帯情報端末２０ｐからの情報の獲得を

する論理回路である。又、認証用画像コード生成手段（モジュール）３４２は、認証用画像コードの生成をする論理回路である。更に、画像データ送信手段（モジュール）３４３は、認証用画像コードを画像データとして第１携帯情報端末２０ｐに送信する論理回路であり、第２携帯情報端末情報獲得手段（モジュール）３４４は、第２携帯情報端末２０ｑからの認証用画像コード内の情報と第２携帯情報端末２０ｑの機体情報の受信をする論理回路であり、情報編集手段（モジュール）３４５は、第２携帯情報端末２０ｑの機体情報による第１携帯情報端末２０ｐの情報の編集をする論理回路である。そして、編集情報送信手段（モジュール）３４６は、第２携帯情報端末２０ｑに第１携帯情報端末２０ｐの情報を送信する論理回路である。又、第１２の実施例に係る情報処理システムと同様に、事業者情報登録装置３７は、事業者情報を記憶する記憶装置で、個人情報登録装置３８は、認証対象となる個人情報記憶する記憶装置である。

図３７のフローチャートを用いて、本発明の第１４の実施例に係る情報処理方法を説明する。ここでは第１携帯情報端末２０ｐから第２携帯情報端末２０ｑにデータを受け渡す場合の流れを仮定する：

（ａ）まず、ステップＳ７４１において、紙媒体等に印刷された事業用画像コードを第１携帯情報端末２０ｐの画像コード読取装置１９ｐが撮影し、画像データ記憶

装置１２ｐに格納する。第１携帯情報端末２０ｐの画像取込手段（モジュール）１１ｐは、画像データ記憶装置１２ｐから事業用画像コードを取り込み、この事業用画像コードに含まれる情報を画像コード解読手段（モジュール）１３ｑにより解読し、解読された情報と個人情報記憶装置１８ｐに記憶された個人情報とを統合データ編集手段（モジュール）１６ｐが編集統合し、第１統合情報を作成する。そして、第１携帯情報端末２０ｐは、この第１統合情報を、仲介サーバである情報処理サーバ３０に送信する。

（ｂ）ステップＳ７４２においては、情報処理サーバ３０が第１携帯情報端末２０ｐからの第１統合情報を獲得し，認証用画像コードを生成し，画像データとして第１携帯情報端末２０ｐに送信する。すると、ステップＳ７４３において、第１携帯情報端末２０ｐの画像表示装置１５ｐの画面上に認証用画像コードが表示される．

（ｃ）ステップＳ７４４において、第１携帯情報端末２０ｐの画像表示装置１５ｐに表示された認証用画像コードを第２携帯情報端末２０ｑの画像コード読取装置１９ｑが撮影し、これを画像データ記憶装置１２ｑに格納する。第２携帯情報端末２０ｑの画像取込手段（モジュール）１１ｑは、画像データ記憶装置１２ｑから認証用画像コードを取り込み、この認証用画像コードに含まれる情報を画像コード解読手段（モジュール）１３ｑにより解読し、解読された情報と個人情報記憶装置１８ｑに

記憶された機体情報とを統合データ編集手段（モジュール）１６ｑが編集統合し、第２統合情報を作成する。

（ｄ）ステップＳ７４５においては、第２携帯情報端末２０ｑから情報処理サーバ３０へ第２統合情報が送信される。ステップＳ７４６では、情報処理サーバ３０において、第２携帯情報端末２０ｑの機体情報を用い、第１携帯情報端末２０ｐの情報を整え，第２携帯情報端末２０ｑに送信する。即ち、第２携帯情報端末２０ｑに第１携帯情報端末２０ｐからの情報を送信する。

図３８は、第１４の実施例に係る情報処理方法の実施に用いる情報処理サーバ３０の動作を説明するフローチャートである：

（ａ）第１携帯情報端末２０ｐがこの第１統合情報を情報処理サーバ３０に送信すると、ステップＳ７５１において、情報処理サーバ３０の第１携帯情報端末情報獲得手段（モジュール）３４１が、第１携帯情報端末２０ｐからの第１統合情報の獲得をする。

（ｂ）次に、ステップＳ７５２において、情報処理サーバ３０の認証用画像コード生成手段（モジュール）３４２は、認証用画像コードの生成をする。

（ｃ）そして、ステップＳ７５３において、情報処理サーバ３０の画像データ送信手段（モジュール）３４３は、認証用画像コードを画像データとして第１携帯情報端末２０ｐに送信する。

（ｄ）第１携帯情報端末２０ｐに表示された認証用画像コードを第２携帯情報端末２０ｑが撮影し、第２携帯情報端末２０ｑから情報処理サーバ３０へ第２統合情報が送信されるト、ステップＳ７５４において、情報処理サーバ３０の第２携帯情報端末情報獲得手段（モジュール）３４４ガ、第２携帯情報端末２０ｑからの第２統合情報に含まれる認証用画像コード内の情報と第２携帯情報端末２０ｑの機体情報の受信をする。

（ｅ）その後、ステップＳ７５５において、情報処理サーバ３０の情報編集手段（モジュール）３４５は、第２携帯情報端末２０ｑの機体情報による第１携帯情報端末２０ｐの情報の編集をする。

（ｆ）次に、ステップＳ７５６において、情報処理サーバ３０の編集情報送信手段（モジュール）３４６は、第２携帯情報端末２０ｑに第１携帯情報端末２０ｐの情報を送信する。

＜第１４の実施例の第１変形例：特定情報交換＞

図３９に示す方式で第１携帯情報端末２０ｓの特定情報を第２携帯情報端末２０ｔの携帯電話の取得する：

（ａ）まず、ステップＳ９０１において、紙媒体等に印刷された事業用画像コードを第１携帯情報端末２０ｓの画像コード読取装置が撮影し、画像データ記憶装置に格納する。第１携帯情報端末２０ｓの画像取込手段（モジュール）は、画像データ記憶装置から事業用画像コー

ドを取り込み、この事業用画像コードに含まれる情報を画像コード解読手段（モジュール）により解読し、解読された情報と個人情報記憶装置に記憶された個人情報とを統合データ編集手段（モジュール）が編集統合し、第１統合情報を作成する。第１統合情報には、第１携帯情報端末２０ｓから第２携帯情報端末２０ｔに登録させたい特定情報も含ませる。そして、ステップＳ９０２において、第１携帯情報端末２０ｓは、この第１統合情報を、仲介サーバである情報処理サーバ３０に送信する。

（ｂ）ステップＳ９０３において、情報処理サーバ３０が第１携帯情報端末２０ｓからの第１統合情報を獲得し，特定情報（例えば電話帳登録情報）を画像コードに生成する。ステップＳ９０４において特定情報の画像コードを，画像データとして第１携帯情報端末２０ｓに送信する。すると、ステップＳ９０５において、第１携帯情報端末２０ｓの画像表示装置の画面上に特定情報の画像データが表示される．

（ｃ）ステップＳ９０５において、第１携帯情報端末２０ｓの画像表示装置に表示された特定情報の画像データ（電話帳登録情報）を第２携帯情報端末２０ｔの画像コード読取装置が撮影し、これを画像データ記憶装置に格納する。第２携帯情報端末２０ｔの画像取込手段（モジュール）は、画像データ記憶装置から特定情報の画像データ（電話帳登録情報）を取り込み、この特定情報の画像データ（電話帳登録情報）に含まれる情報を画像コ

ード解読手段（モジュール）により解読し、解読された特定情報と個人情報記憶装置に記憶された機体情報とを統合データ編集手段（モジュール）が編集統合し、第２統合情報を作成する。

（ｄ）ステップＳ９０６においては、第２携帯情報端末２０ｔから情報処理サーバ３０へ第２統合情報が送信される。ステップＳ９０７では、情報処理サーバ３０において、第２携帯情報端末２０ｔの機体情報を用い、第１携帯情報端末２０ｓの特定情報（電話帳登録情報）を整え，ステップＳ９０８において第２携帯情報端末２０ｔに送信する。即ち、第２携帯情報端末２０ｔに第１携帯情報端末２０ｓからの特定情報（電話帳登録情報）をステップＳ９０８において送信する。場合によってはパーソナルコンピュータ２０ｚなどの別機体に第１携帯情報端末２０ｓからの特定情報（電話帳登録情報）を同時送信しても良い。

なお、必要であれば、第２携帯情報端末２０ｔの特定情報の画像コードを発行し第１携帯情報端末２０ｓの携帯電話で読ませることで情報交換させる（手順は同じだが、相手の携帯機種が分かっているので、相手の携帯電話用の画像コードを作成し表示して読ませれば良い）。

＜第１４の実施例の第２変形例：所有者の相性占い＞

二次元コードの情報（アクション情報），第１携帯情報端末２０ｓの情報（個人情報），第２携帯情報端末２

０ｔの情報（個人情報）に起因したアクションを実現できる．つまり，２つ以上の個人情報によるアクションが実現できる．例えば，第１携帯情報端末２０ｓの所有者と第２携帯情報端末２０ｔの所有者の相性占いなどが挙げられる．図４０は、第１携帯情報端末２０ｓの所有者と第２携帯情報端末２０ｔの所有者の相性占いを想定している：

（ａ）まず、ステップＳ９１１において、紙媒体等に印刷された相性占いコードを第１携帯情報端末２０ｓの画像コード読取装置が撮影し、画像データ記憶装置に格納する。第１携帯情報端末２０ｓの画像取込手段（モジュール）は、画像データ記憶装置から相性占いコードを取り込み、この相性占いコードに含まれる情報を画像コード解読手段（モジュール）により解読し、解読された情報と個人情報記憶装置に記憶された個人情報とを統合データ編集手段（モジュール）が編集統合し、第１統合情報を作成する。第１統合情報には、第１携帯情報端末２０ｓから第２携帯情報端末２０ｔに登録させたいアクション情報も含ませる。そして、ステップＳ９１２において、第１携帯情報端末２０ｓは、この第１統合情報を、仲介サーバである情報処理サーバ３０に送信する。

（ｂ）ステップＳ９１３において、情報処理サーバ３０が第１携帯情報端末２０ｓからの第１統合情報を獲得し，アクション情報を画像コードに生成する。ステップＳ９１４においてアクション情報（第２携帯情報端末２

０ｔに読ませたい占い情報）の画像コードを，画像データとして第１携帯情報端末２０ｓに送信する。すると、ステップＳ９１５において、第１携帯情報端末２０ｓの画像表示装置の画面上にアクション情報の画像データが表示される．

（ｃ）ステップＳ９１５において、第１携帯情報端末２０ｓの画像表示装置に表示されたアクション情報の画像データを第２携帯情報端末２０ｔの画像コード読取装置が撮影し、これを画像データ記憶装置に格納する。第２携帯情報端末２０ｔの画像取込手段(モジュール)は、画像データ記憶装置からアクション情報の画像データを取り込み、このアクション情報の画像データに含まれる情報を画像コード解読手段(モジュール)により解読し、解読されたアクション情報と個人情報記憶装置に記憶された機体情報とを統合データ編集手段（モジュール）が編集統合し、第２統合情報を作成する。

（ｄ）ステップＳ９１６においては、第２携帯情報端末２０ｔから情報処理サーバ３０へ第２統合情報が送信される。ステップＳ９１７では、情報処理サーバ３０において、第２携帯情報端末２０ｔの機体情報を用い、第１携帯情報端末２０ｓのアクション情報を整え，第１携帯情報端末２０ｓの所有者と第２携帯情報端末２０ｔの所有者の相性占いを行う。ステップＳ９１８において、第１携帯情報端末２０ｓの所有者と第２携帯情報端末２０ｔの所有者の相性占いの結果は、第２携帯情報端末２

０ｔに送信される。場合によってはパーソナルコンピュータ２０ｚなどの別機体に第１携帯情報端末２０ｓからの第１携帯情報端末２０ｓの所有者と第２携帯情報端末２０ｔの所有者の相性占いの結果を同時送信しても良い。

＜第１４の実施例の第３変形例：パーミッション機能を伴う情報共有＞

複数、即ち、第１携帯情報端末２０ｓ、第２携帯情報端末２０ｔ、第３携帯情報端末２０ｕ、第４携帯情報端末２０ｖの４台の端末があるとする。この４台の端末中の第１携帯情報端末２０ｓ、第２携帯情報端末２０ｔ及び第４携帯情報端末２０ｖの３台の端末のみ情報が共有され、第３携帯情報端末２０ｕには情報が共有できないように、パーミッション機能を設定して特定の端末にのみ情報が共有されるようにするシステムである。

（ａ）まず、情報処理サーバ３０において、第１携帯情報端末２０ｓからアクションがあっとき、第２携帯情報端末２０ｔ及び第４携帯情報端末２０ｖのみにそのアクションを許可するように設定しておく。

（ｂ）次に、ステップＳ９２１において、第１携帯情報端末２０ｓの画像表示装置に表示された特定の情報の画像データを第２携帯情報端末２０ｔの画像コード読取装置が撮影し、この特定の情報の画像データに含まれる情報を画像コード解読手段（モジュール）により解読し、解読された特定の情報と第２携帯情報端末２０ｔの個人

情報記憶装置に記憶された機体情報とを統合データ編集手段（モジュール）が編集統合し、第２携帯情報端末２０ｔの統合情報を作成する。そして、第２携帯情報端末２０ｔから第２携帯情報端末２０ｔの統合情報を情報処理サーバ３０へ送信する。

（ｃ）情報処理サーバ３０において、第２携帯情報端末２０ｔに対してアクションが許可されているのを確認し、第２携帯情報端末２０ｔの機体情報を用い、第１携帯情報端末２０ｓの特定の情報を整える。そして、ステップＳ９２２において、第１携帯情報端末２０ｐから得られた特定の情報は、第２携帯情報端末２０ｔに第２携帯情報端末２０ｔの機体に合致した形式で、送信される。

（ｄ）次に、ステップＳ９２３において、第１携帯情報端末２０ｓの画像表示装置に表示された特定の情報の画像データを第３携帯情報端末２０ｕの画像コード読取装置が撮影し、この特定の情報の画像データに含まれる情報を画像コード解読手段（モジュール）により解読し、解読された特定の情報と第３携帯情報端末２０ｕの個人情報記憶装置に記憶された機体情報とを統合データ編集手段（モジュール）が編集統合し、第３携帯情報端末２０ｕの統合情報を作成する。そして、第３携帯情報端末２０ｕから第３携帯情報端末２０ｕの統合情報を情報処理サーバ３０へ送信したとする。

（ｅ）しかし、情報処理サーバ３０においては、第３携帯情報端末２０ｕに対してアクションが許可されてい

ないので、第３携帯情報端末２０ｕの機体情報を用い、第１携帯情報端末２０ｓの特定の情報を整えることができない。このため、ステップＳ９２４において、第１携帯情報端末２０ｐから得られた特定の情報は、第３携帯情報端末２０ｕに送信できず、エラーが送信される。

（ｆ）更に、第１携帯情報端末２０ｓの画像表示装置に表示された特定の情報の画像データを第４携帯情報端末２０ｖの画像コード読取装置が撮影し、解読された特定の情報と第４携帯情報端末２０ｖの個人情報記憶装置に記憶された機体情報との統合情報が作成され、情報処理サーバ３０へ送信されれば、情報処理サーバ３０においては、第４携帯情報端末２０ｖに対してアクションが許可されているのを確認し、第４携帯情報端末２０ｖの機体情報を用い、第１携帯情報端末２０ｓの特定の情報を整えることができる。そして、その後、第１携帯情報端末２０ｐから得られた特定の情報は、第４携帯情報端末２０ｖに第４携帯情報端末２０ｖの機体に合致した形式で送信される。

この様にして、第１携帯情報端末２０ｓの特定の情報のみが、第２携帯情報端末２０ｔ及び第４携帯情報端末２０ｖに送られ、第３携帯情報端末２０ｕには送信できなくなる。情報が共有できないように、パーミッション機能を設定して特定の端末にのみ情報が共有されるようにするシステムである

第１４の実施例の第３変形例に係る情報処理システム

のパーミッション機能は、タイムスタンプによって設定しても良い。更に、も考えられる。なお、第１４の実施例の第３変形例に係る情報処理システムは、自作の着メロ交換など携帯情報端末によって依存するものに効果的である。

＜第１４の実施例の第４変形例：コンテンツ同期方式＞

２台以上の携帯情報端末（携帯電話）で、違うコンテンツ、例えば音声・音楽ファイルをダウンロードし、同時に再生を行うことによって、ＢＧＭと朗読、伴奏と主旋律、ＪＡＭセッションなどを実現する。このとき、ＪＡＭセッションなどは、携帯情報端末（携帯電話）の同期が必要になる。

第１４の実施例の第４変形例に係る情報処理方法においては、各携帯情報端末（携帯電話）は、絶対時間を持っており、それらは共通化されている。例えば電波時計などで合わせたり、どこかのサーバに時刻情報があったり、それに同期したクロックを持っている。（或いは、画像コードを読んだとき、クロック（時刻）情報を当該サーバから読込んでも良い。）。各携帯情報端末は、同時演奏マークを読むと、開始タイミングが指定され、ほぼ、同時（１，２秒ずれても良い）に演奏開始すると、先のクロックに同期し同時に演奏が始まる。例えば、最も近い、３０秒刻みの、時刻に開始するなど、小節毎に同期を取ることも可能。又、ＭＩＤＩと連動させても良

い。

（その他の実施例）

上記のように、本発明は第１乃至第１４の実施例によって記載したが、この開示の一部をなす論述及び図面はこの発明を限定するものであると理解すべきではない。この開示から当業者には様々な代替実施例及び運用技術が明らかとなろう。

第１～第３の実施例においては、第１のウェアラブルコンピュータ（携帯情報端末）１０ａから送信元メタデータＭＤ０を発生させる流れを例示したが、事業者サーバ５１等側からメタデータを生成してユーザ側に送信されるような逆の流れで個人情報保護方式を利用しても同様のセキュリティを確保することができる。

又、複数のコミュニティに属する場合に、発信者はどのコミュニティに対して送信しているのかを、第１のウェアラブルコンピュータ１０ａの入力部位から指定したり、ＳＩＭカード、ＩＣチップ又はＲＦＩＤ等を差し替えたり、第１のウェアラブルコンピュータ１０ａによってスキャンするコード等に埋め込んでおいて識別したり様々な方法を選択しても構わない。

第４～第６の実施例においては、第１のウェアラブルコンピュータ１０ａから送信元メタデータＭＤ０を発生させる流れを例示したが、事業者サーバ５１等側からメ

タデータを生成してユーザ側に送信されるような逆の流れで個人情報保護方式を利用しても同様のセキュリティを確保することができる。

又、複数のコミュニティに属する場合に、発信者はどのコミュニティに対して送信しているのかを、第１のウェアラブルコンピュータ１０ａの入力部位から指定したり、ＳＩＭカード、ＩＣチップ又はＲＦＩＤ等を差し替えたり、第１のウェアラブルコンピュータ１０ａによってスキャンするコード等に埋め込んでおいて識別したり様々な方法を選択しても構わない。

又、第７～第１１の実施例で説明した第１のウェアラブルコンピュータ１０ａで生成された検索タグ情報ＣＯＤＥを用いる暗号化鍵取得方法を、第２の実施例で説明される電子商取引や、第３の実施例で説明されるコミュニティ内の情報交換における情報保護方式に用いることも可能である。

第７～第１１の実施例で説明した検索タグ情報ＣＯＤＥ２は、暗号化して送信されると説明しているが、暗号化プロトコルＳＳＬ等を用いた暗号通信方法を用いる場合は暗号化せずに検索タグ情報ＣＯＤＥ２をそのまま送信することが可能である。

例えば、通信端末へ情報を送信すると同時に、パーソナルコンピュータ等の別の機体にも情報を送るように、送信先情報を付加して情報処理サーバ３０ａ、３０ｂに画像を送信することも可能である。

この様に、本発明はここでは記載していない様々な実施例等を含むことは勿論である。したがって、本発明の技術的範囲は上記の説明から妥当な請求の範囲記載に係る発明を特定するために必要と認める事項によってのみ定められるものである。なお、２００２年５月３１日に出願された特願２００２－１６０３６９号の開示内容の全体、２００２年７月３０日に出願された特願２００２－２２２１８３号の開示内容の全体、２００３年８月２９日に出願された特願２００３－３０７８７２号の開示内容の全体、及び２００３年９月２９日に出願された特願２００３－３３８６２４号の開示内容の全体は、それぞれ参照により本明細書に挿入されたものとする。

産業上の利用可能性

本発明は、ユビキタス環境下における通信において、個人情報等のデータを当事者以外から秘匿して、種々の電子商取引の分野に適用可能である。更に、イベント会場等の入場管理の分野にも適用できる。

請求の範囲

1．　認証端末が備える認証情報を利用して、認証情報を備えない通信端末を認証する情報処理システムに用いられる情報処理サーバにおいて、

前記認証情報を記憶した認証情報記憶装置と、

前記通信端末の認証依頼を受信すると、認証パラメータを生成し、前記認証パラメータを含む認証画像を生成して前記通信端末に送信し、前記認証パラメータを認証パラメータ記憶装置に記憶する認証画像生成モジュールと、

前記通信端末から取得した前記認証画像の情報と、前記認証端末が備える前記認証情報を、前記認証端末から取得する認証情報取得モジュールと、

前記認証パラメータ記憶装置を参照して、前記認証情報取得モジュールで取得した前記認証画像の情報が、前記認証画像生成モジュールで生成された画像の情報であり、更に、前記認証端末が備える前記認証情報が、前記認証情報記憶装置に記憶した前記認証情報と一致するか否かを判定し、その結果を前記通信端末に送信する認証情報照合モジュール

とを備えることを特徴とする情報処理サーバ。

2．　前記認証画像生成モジュールで生成する認証パラメータは、一意に特定できる乱数及び日時のいずれか1つ以上を含むことを特徴とする請求の範囲第1項に記載

の情報処理サーバ。

３．　前記認証画像生成モジュールにおいて、前記認証パラメータ記憶装置に、前記認証パラメータの有効日時を更に記憶し、

前記認証情報照合モジュールにおいて、前記認証情報取得モジュールによって取得した日時が、前記認証パラメータ記憶装置に記憶された前記認証パラメータの有効日時以前の場合に認証を許可し、前記認証パラメータの有効日時以降の場合に認証を不可にする

ことを特徴とする請求の範囲第１項に記載の情報処理サーバ。

４．　前記認証画像生成モジュールにおいて、第１の通信ネットワークを利用して前記通信端末に前記認証画像を送信し、

前記認証情報取得モジュールにおいて、前記第１の通信ネットワークとは異なる第２の通信ネットワークを利用して前記認証端末から前記認証画像の情報と前記認証情報を取得する

ことを特徴とする請求の範囲第１項に記載の情報処理サーバ。

５．　前記認証画像の情報は、前記通信端末から取得した前記認証画像を、前記認証端末においてデコードした

情報であることを特徴とする請求の範囲第１項に記載の情報処理サーバ。

６．　前記認証画像の情報は、前記通信端末から取得し、前記認証端末から受信した前記認証画像を、デコードした情報であることを特徴とする請求の範囲第１項に記載の情報処理サーバ。

７．　前記通信端末から前記認証画像の情報を取得する場合、前記認証端末によって、前記通信端末に提示された認証画像を撮影しデコードすることを特徴とする請求の範囲第１項に記載の情報処理サーバ。

８．　前記情報処理システムは、前記通信端末にコンテンツを提供するコンテンツ提供サーバを更に備えており、
前記認証画像生成モジュールにおいて、前記コンテンツ提供サーバから、前記通信端末の認証依頼を受信し、
前記認証情報照合モジュールにおいて、前記結果を前記コンテンツ提供サーバに送信する
ことを特徴とする請求の範囲第１項に記載の情報処理サーバ。

９．　認証端末が備える認証情報を利用して、認証情報を備えない通信端末を認証する情報処理システムに用いられる情報処理方法において、

前記認証情報を認証情報記憶装置に記憶するステップと、

認証画像生成モジュールによって、前記通信端末の認証依頼を受信すると、認証パラメータを生成し、前記認証パラメータを含む認証画像を生成して前記通信端末に送信し、前記認証パラメータを認証パラメータ記憶装置に記憶する前記認証画像を生成するステップと、

認証情報取得モジュールによって、前記認証端末から、前記通信端末から取得した前記認証画像の情報と、前記認証端末が備える前記認証情報を取得するステップと、

認証情報照合モジュールによって、前記認証パラメータ記憶装置を参照して、前記認証画像の情報が、前記認証画像を生成するステップで生成された画像の情報であり、更に、前記認証端末が備える前記認証情報が、前記認証情報記憶装置に記憶した前記認証情報と一致するか否かを判定し、その結果を前記通信端末に送信する前記認証情報を照合するステップ

とを備えることを特徴とする情報処理方法。

１０．　前記認証画像を生成するステップで生成する認証パラメータは、一意に特定できる乱数及び日時のいずれか１つ以上を含むことを特徴とする請求の範囲第９項に記載の情報処理方法。

１１．　前記認証画像を生成するステップにおいて、

前記認証パラメータ記憶装置に、前記認証パラメータの有効日時を更に記憶し、

前記認証情報を照合するステップにおいて、前記認証情報を取得するステップによって取得した日時が、前記認証パラメータ記憶装置に記憶された前記認証パラメータの有効日時以前の場合に認証を許可し、前記認証パラメータの有効日時以降の場合に認証を不可にする

ことを特徴とする請求の範囲第９項に記載の情報処理方法。

１２．　前記認証画像を生成するステップにおいて、第１の通信ネットワークを利用して前記通信端末に前記認証画像を送信し、

前記認証情報を取得するステップにおいて、前記第１の通信ネットワークとは異なる第２の通信ネットワークを利用して前記認証端末から前記認証画像の情報と前記認証情報を取得する

ことを特徴とする請求の範囲第９に記載の情報処理方法。

１３．　前記認証画像の情報は、前記通信端末から取得した前記認証画像を、前記認証端末においてデコードした情報であることを特徴とする請求の範囲第９項に記載の情報処理方法。

１４．　前記認証画像の情報は、前記通信端末から取得し、前記認証端末から受信した前記認証画像を、デコードした情報であることを特徴とする請求の範囲第９項に記載の情報処理方法。

１５．　前記通信端末から前記認証画像の情報を取得する場合、前記認証端末によって、前記通信端末に提示された認証画像を撮影しデコードすることを特徴とする請求の範囲第９項に記載の情報処理方法。

１６．　前記情報処理システムは、前記通信端末にコンテンツを提供するコンテンツ提供サーバを更に備えており、

前記認証画像を生成するステップにおいて、前記コンテンツ提供サーバから、前記通信端末の認証依頼を受信し、

前記認証情報を照合するステップにおいて、前記結果を前記コンテンツ提供サーバに送信する

ことを特徴とする請求の範囲第９項に記載の情報処理方法。

１７．　通信端末識別子によって検索される対応情報を格納する識別子対応情報記憶装置と、

通信端末から入力される情報を、前記対応情報に従って変換する情報変換モジュール

とを備えることを特徴とする情報処理サーバ。

１８．　前記通信端末から入力される情報から画像を作成する画像作成モジュールを更に備えることを特徴とする請求の範囲第１７項項に記載の情報処理サーバ。

１９．　前記通信端末が情報交換を許可されているか示す許可情報を格納する許可情報記憶装置と、

前記許可情報を判定する許可判定モジュール

とを更に備えることを特徴とする請求の範囲第１７項に記載の情報処理サーバ。

２０．　第１端末、第２端末、及び第１端末と第２端末間を仲介する情報処理サーバとを含むシステムにおいて、

前記情報処理サーバが、

前記第１端末からのアクション要求を、第１レベルの個人情報と共に受信し、

前記第１レベルの個人情報により、前記第１端末を認証し、

前記第１端末に認証情報を発行し、

第１レベルの個人情報よりもセキュリティレベルの高い第２レベルの個人情報を、前記認証情報と共に前記第１端末から受信し、

前記認証情報に基づき、前記アクションに前記第２レベルの個人情報を前記第２端末に送信する

ことを特徴とする情報処理方法。

２１．　前記情報処理サーバは、複数のサーバから構成され、前記第１端末内において、前記複数のサーバの数に対応した複数の情報を、前記複数のサーバに１：１にそれぞれ対応した複数の暗号化鍵でそれぞれ暗号化して、前記複数のサーバの数に対応した複数の暗号化情報を生成して、前記第２レベルの個人情報とし、

前記情報処理サーバが、前記複数のサーバのそれぞれで、前記複数の暗号化情報を順次復号した後、前記第２レベルの個人情報を前記第２端末に送信することを特徴とする請求の範囲第２０項に記載の情報処理方法。

２２．　前記第１レベルの個人情報は、前記第１端末のメモリ内に格納された固定乱数の組により生成されることを特徴とする請求の範囲第２０項に記載の情報処理方法。

２３．前記第１端末は、主第１端末と補助第１端末との組からなり、前記主第１端末に前記認証情報として画像情報を送信し、該画像情報を光学的に読み取った前記補助第１端末の個人情報を、前記第２レベルの個人情報として、前記認証情報と共に前記補助第１端末から受信することを特徴とする請求の範囲第２０項に記載の情報処理方法。

FIG. 1

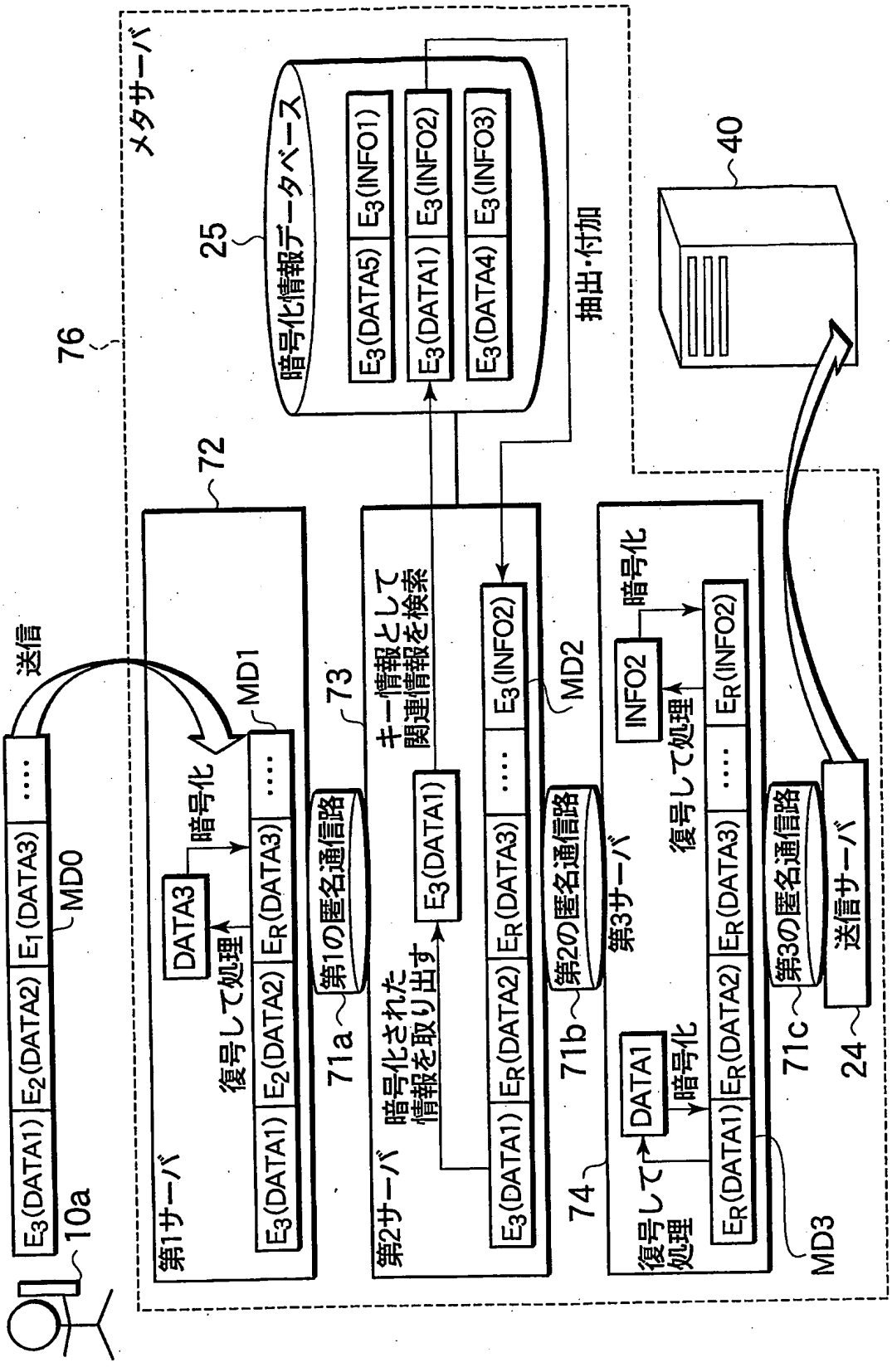

メタサーバ
76
25
暗号化情報データベース
E3(DATA5) E3(INFO1)
E3(DATA1) E3(INFO2)
E3(DATA4) E3(INFO3)
抽出・付加
40
送信
E3(DATA1) E2(DATA2) E1(DATA3) ....
MD0
10a
第1サーバ
72
DATA3
暗号化
復号して処理
MD1
E3(DATA1) E2(DATA2) ER(DATA3) ....
71a
第1の匿名通信路
第2サーバ
73
暗号化された情報を取り出す
E3(DATA1)
キー情報として関連情報を検索
E3(DATA1) ER(DATA2) ER(DATA3) .... E3(INFO2)
MD2
71b
第2の匿名通信路
74
第3サーバ
INFO2
暗号化
復号して処理
DATA1
暗号化
復号して処理
ER(DATA1) ER(DATA2) ER(DATA3) .... ER(INFO2)
MD3
71c
第3の匿名通信路
24
送信サーバ

FIG. 2

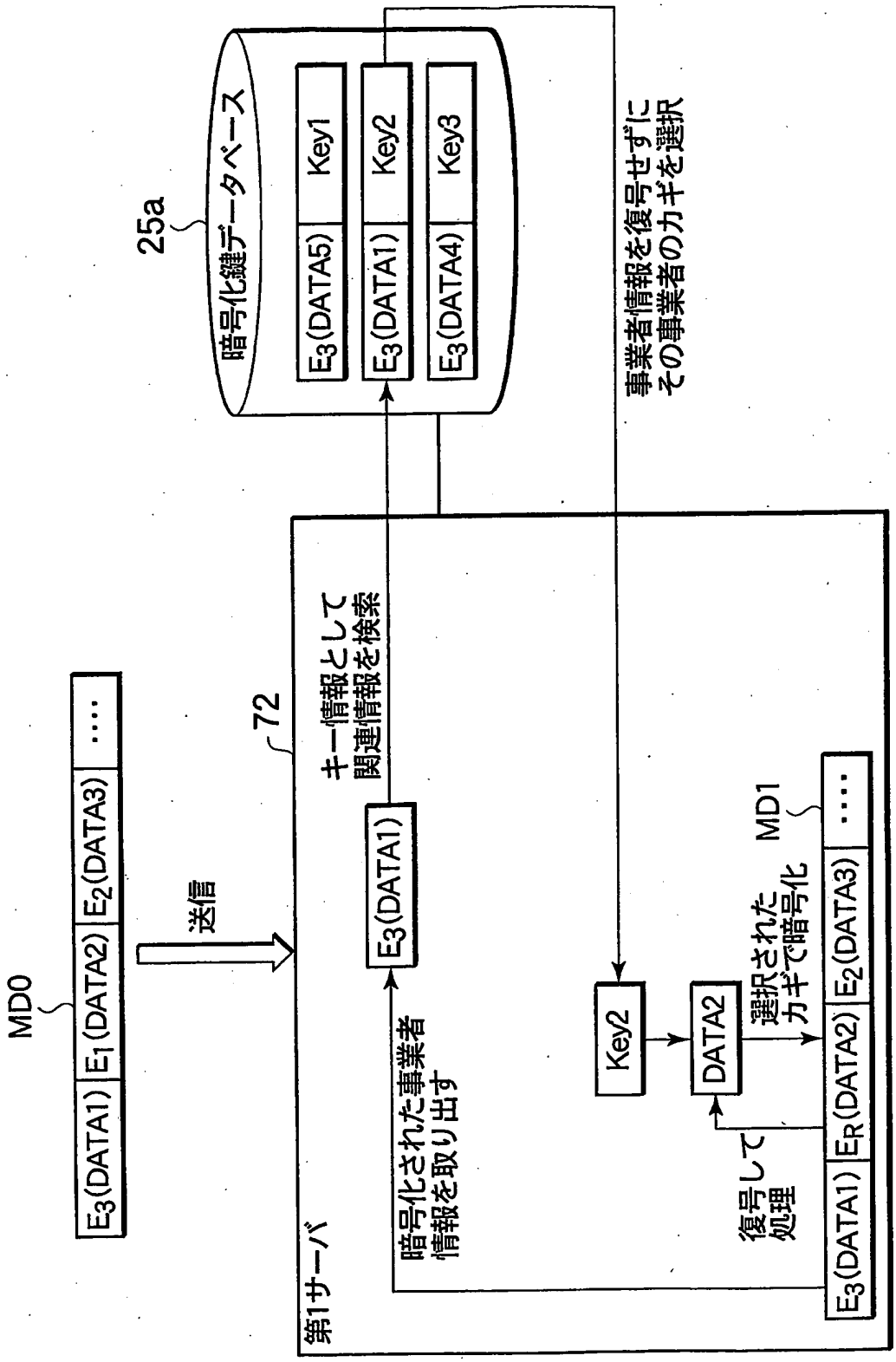

MD0
E3(DATA1) E1(DATA2) E2(DATA3) ....
送信
72
第1サーバ
キー情報として
関連情報を検索
E3(DATA1)
暗号化された事業者
情報を取り出す
25a
暗号化鍵データベース
E3(DATA5) Key1
E3(DATA1) Key2
E3(DATA4) Key3
事業者情報を復号せずに
その事業者のカギを選択
Key2
DATA2
選択された
カギで暗号化
MD1
E3(DATA1) ER(DATA2) E2(DATA3) ....
復号して
処理

FIG. 3

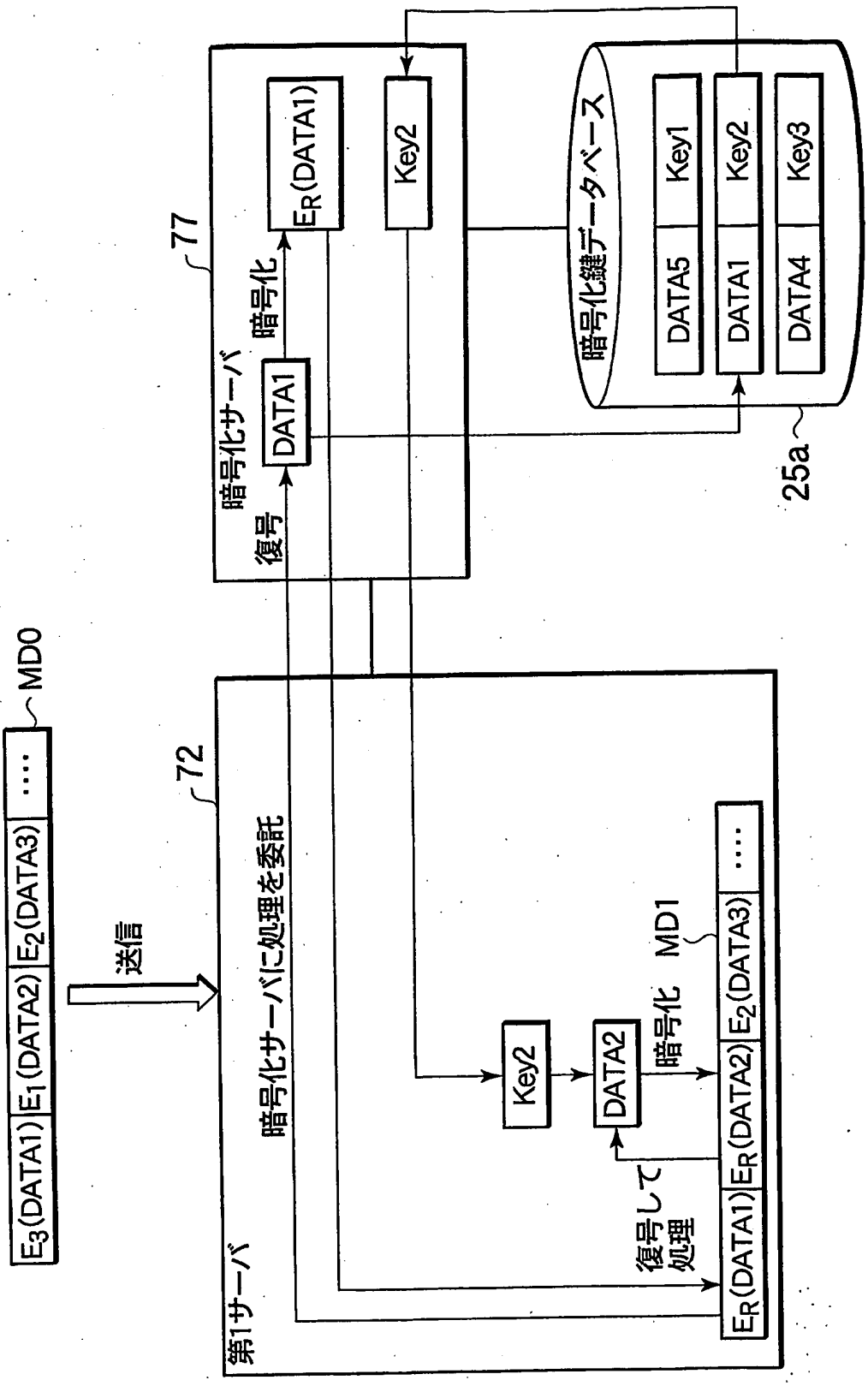

MD0
E3(DATA1)
E1(DATA2)
E2(DATA3)
....
送信
72
第1サーバ
暗号化サーバに処理を委託
77
暗号化サーバ
復号
暗号化
DATA1
ER(DATA1)
Key2
暗号化鍵データベース
DATA5
Key1
DATA1
Key2
DATA4
Key3
25a
Key2
DATA2
暗号化
MD1
ER(DATA1)
ER(DATA2)
E2(DATA3)
....
復号して処理

FIG. 4

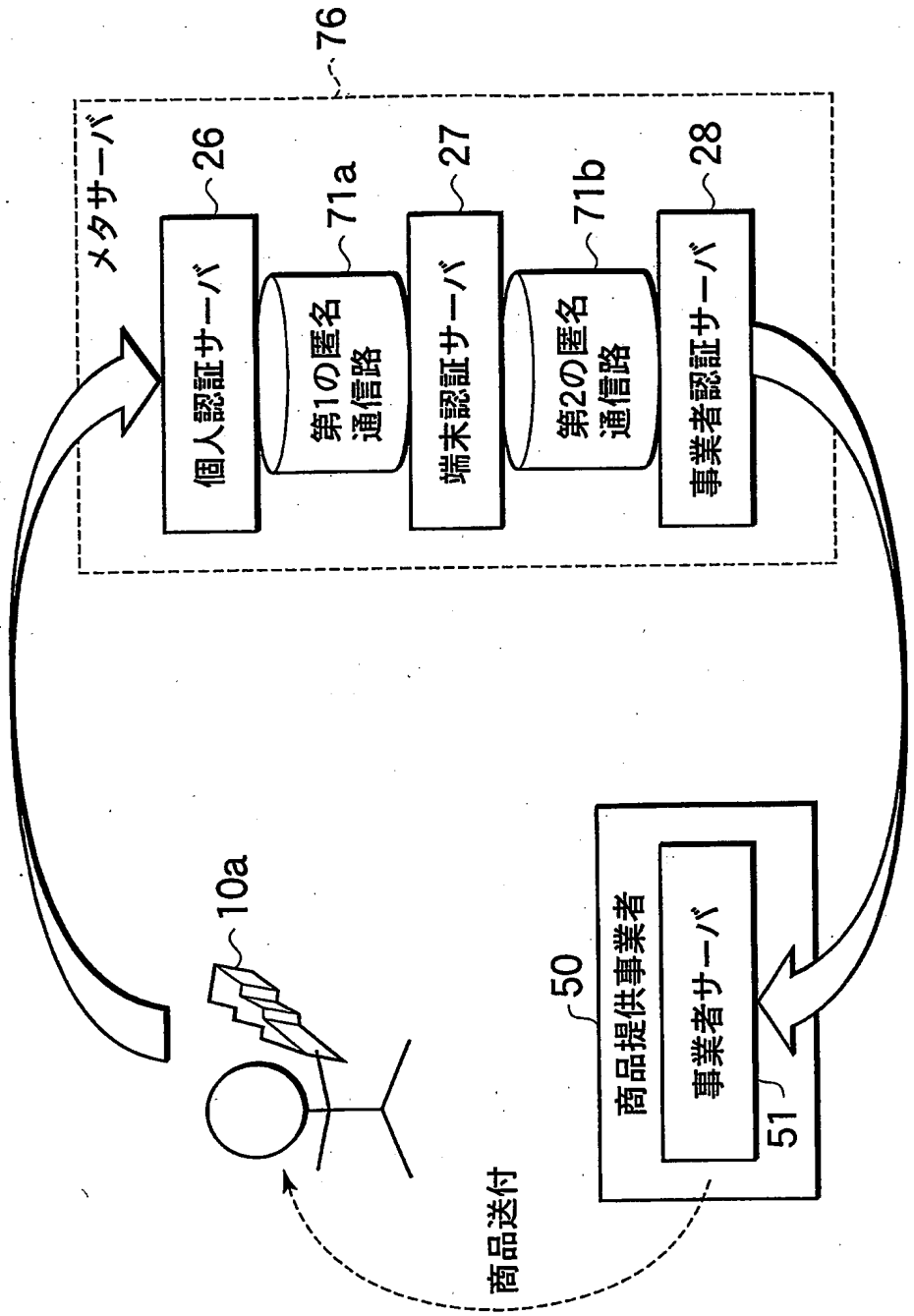

76
メタサーバ
26
個人認証サーバ
71a
第1の匿名通信路
27
端末認証サーバ
71b
第2の匿名通信路
28
事業者認証サーバ
10a
50
商品提供事業者
事業者サーバ
51
商品送付

FIG. 5

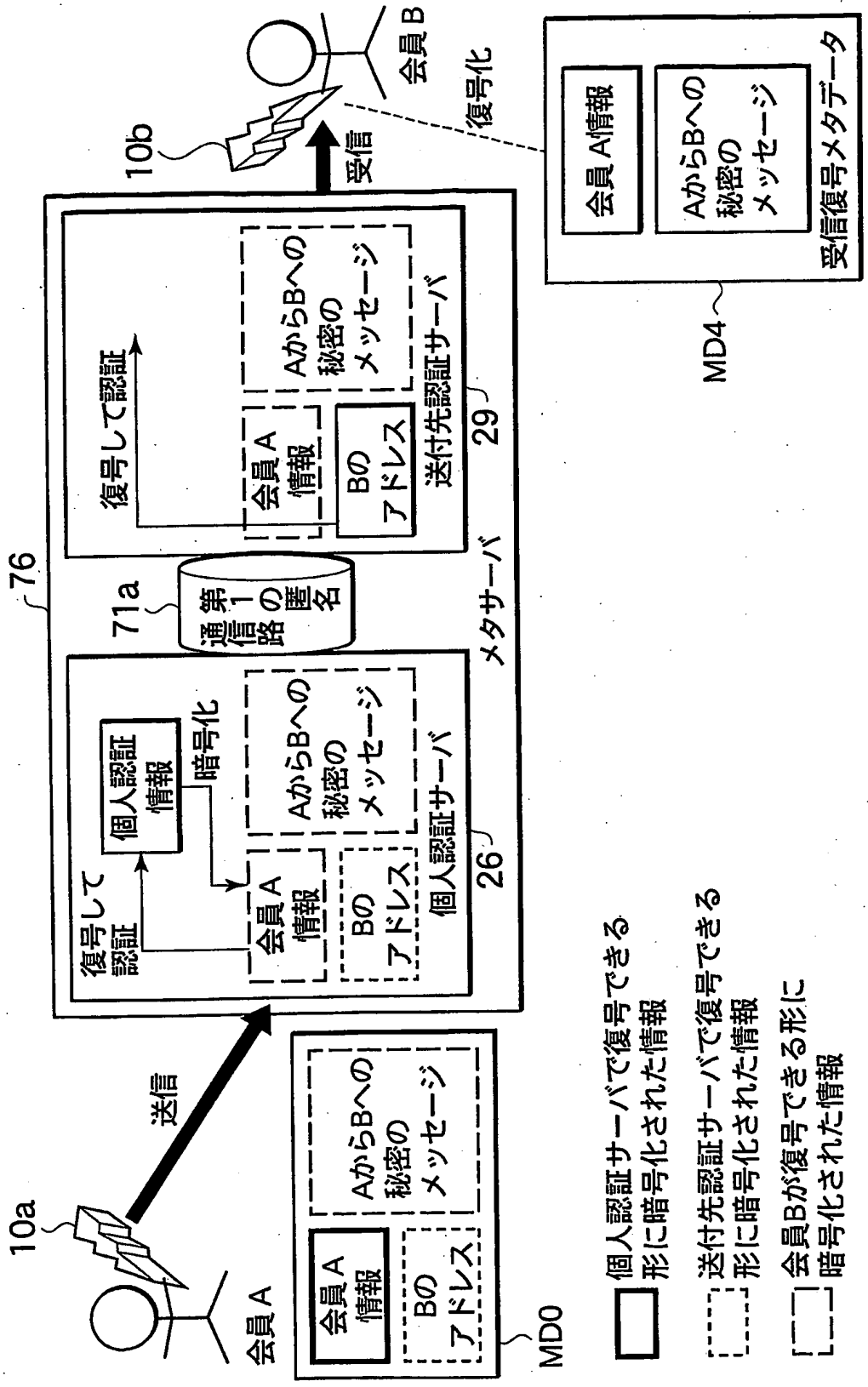

10a
会員A
送信
会員A情報
Bのアドレス
AからBへの秘密のメッセージ
MD0
76
71a
第1の匿名通信路
メタサーバ
復号して認証
個人認証情報
暗号化
会員A情報
Bのアドレス
AからBへの秘密のメッセージ
個人認証サーバ
26
復号して認証
会員A情報
Bのアドレス
AからBへの秘密のメッセージ
送付先認証サーバ
29
10b
受信
会員B
復号化
会員A情報
AからBへの秘密のメッセージ
受信復号メタデータ
MD4
個人認証サーバで復号できる形に暗号化された情報
送付先認証サーバで復号できる形に暗号化された情報
会員Bが復号できる形に暗号化された情報

FIG. 6

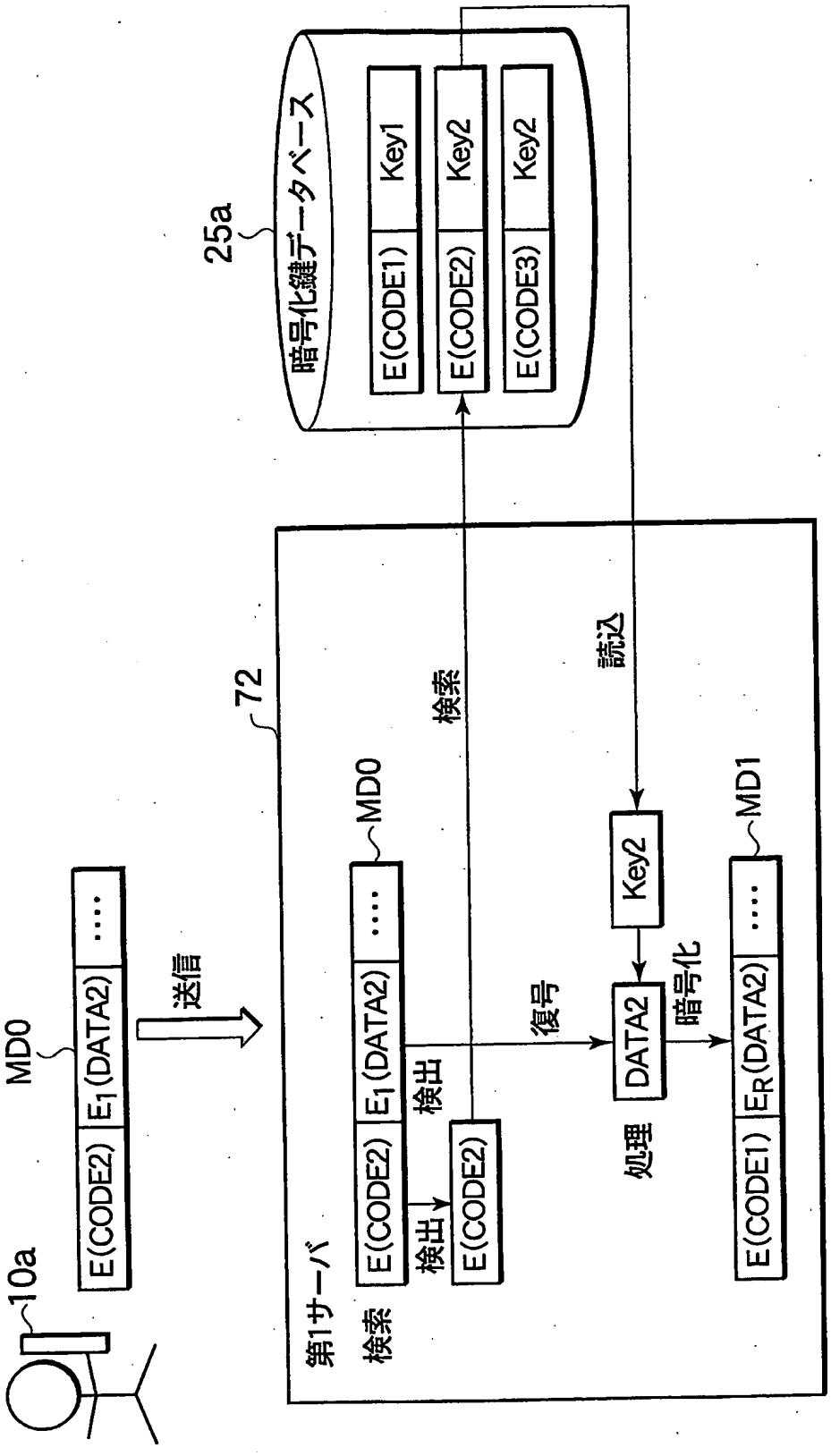

10a
MD0
E(CODE2)
E1(DATA2)
....
送信
72
第1サーバ
検索
E(CODE2)
E1(DATA2)
MD0
検出
E(CODE2)
検索
検出
復号
DATA2
処理
Key2
暗号化
MD1
ER(DATA2)
E(CODE1)
読込
25a
暗号化鍵データベース
E(CODE1)
Key1
E(CODE2)
Key2
E(CODE3)
Key2

FIG. 7

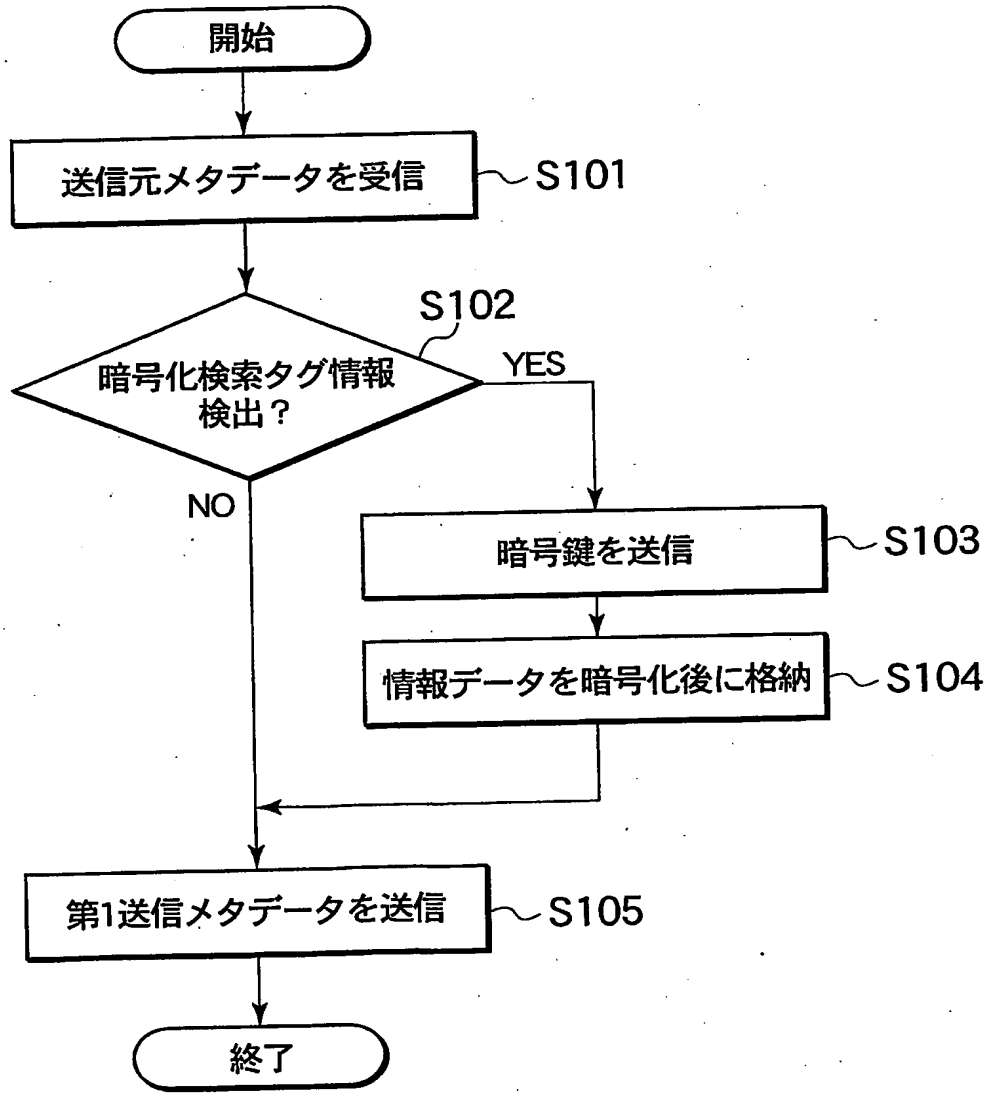

開始
送信元メタデータを受信
S101
S102
暗号化検索タグ情報検出？
YES
NO
暗号鍵を送信
S103
情報データを暗号化後に格納
S104
第1送信メタデータを送信
S105
終了

FIG. 8

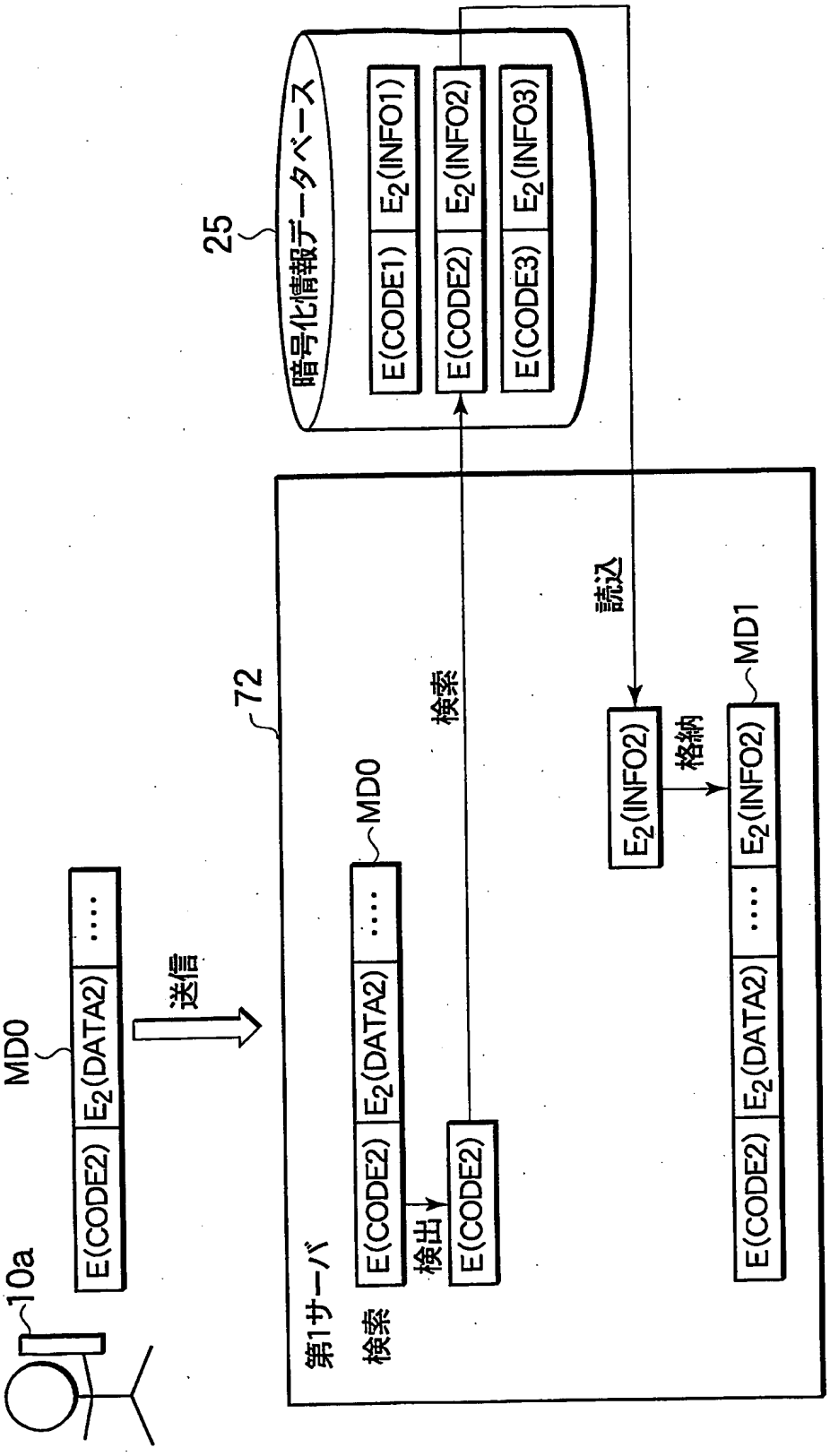

10a
MD0
E(CODE2)
E2(DATA2)
....
送信
72
第1サーバ
検索
MD0
E(CODE2)
E2(DATA2)
....
検出
E(CODE2)
検索
25
暗号化情報データベース
E(CODE1)
E2(INFO1)
E(CODE2)
E2(INFO2)
E(CODE3)
E2(INFO3)
読込
E2(INFO2)
格納
MD1
E(CODE2)
E2(DATA2)
....
E2(INFO2)

FIG. 9

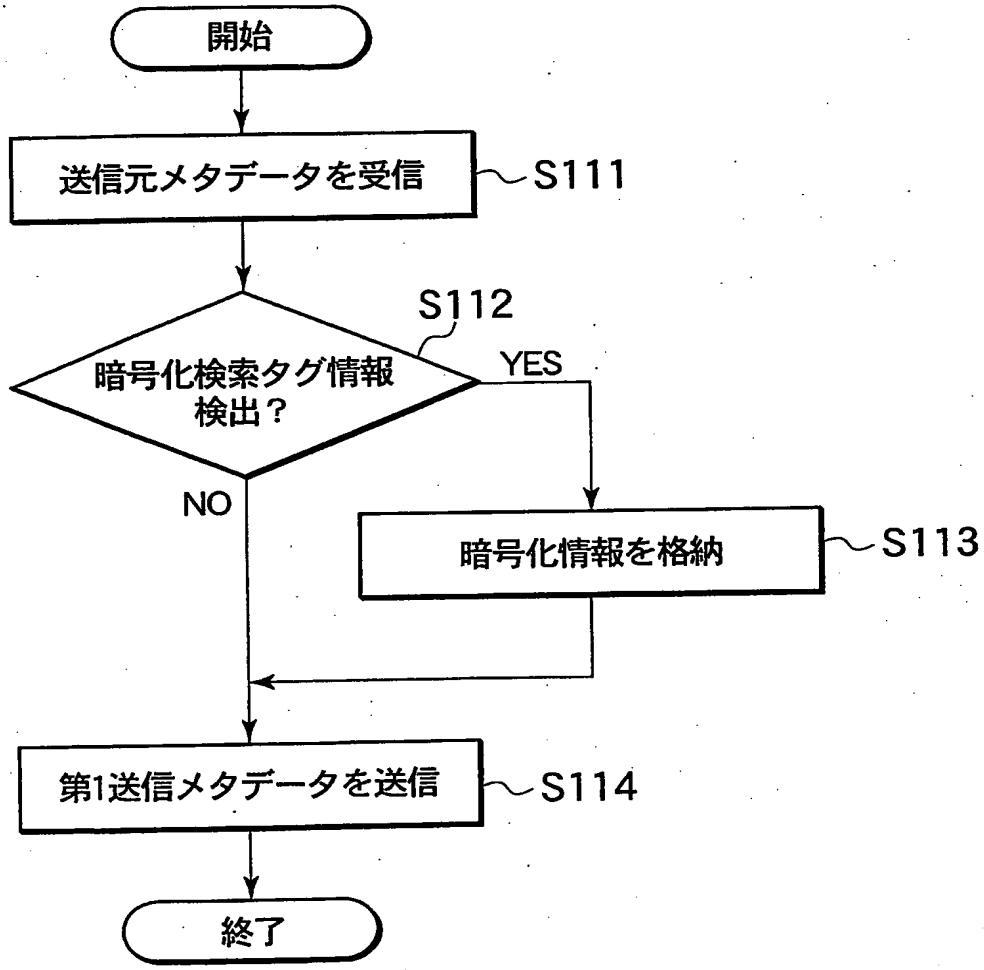

開始
送信元メタデータを受信
S111
S112
暗号化検索タグ情報検出？
YES
NO
暗号化情報を格納
S113
第1送信メタデータを送信
S114
終了

FIG. 10

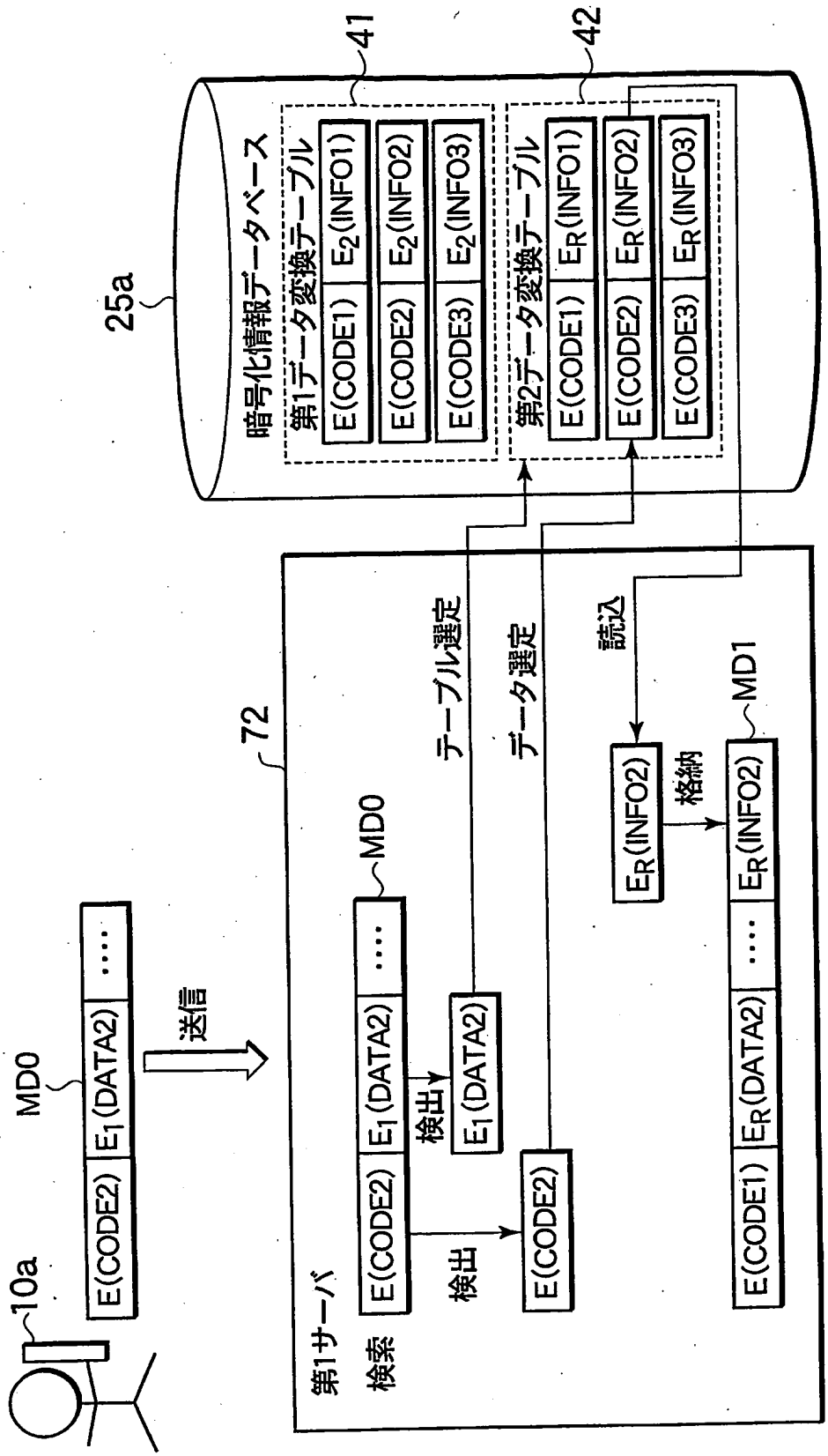

10a
MD0
E(CODE2)
E1(DATA2)
送信
25a
暗号化情報データベース
41
第1データ変換テーブル
E(CODE1) E2(INFO1)
E(CODE2) E2(INFO2)
E(CODE3) E2(INFO3)
42
第2データ変換テーブル
E(CODE1) ER(INFO1)
E(CODE2) ER(INFO2)
E(CODE3) ER(INFO3)
72
第1サーバ
検索
MD0
E(CODE2) E1(DATA2)
検出
E1(DATA2)
テーブル選定
データ選定
検出
E(CODE2)
読込
ER(INFO2)
格納
MD1
ER(INFO2)
E(CODE1) ER(DATA2)

FIG. 11

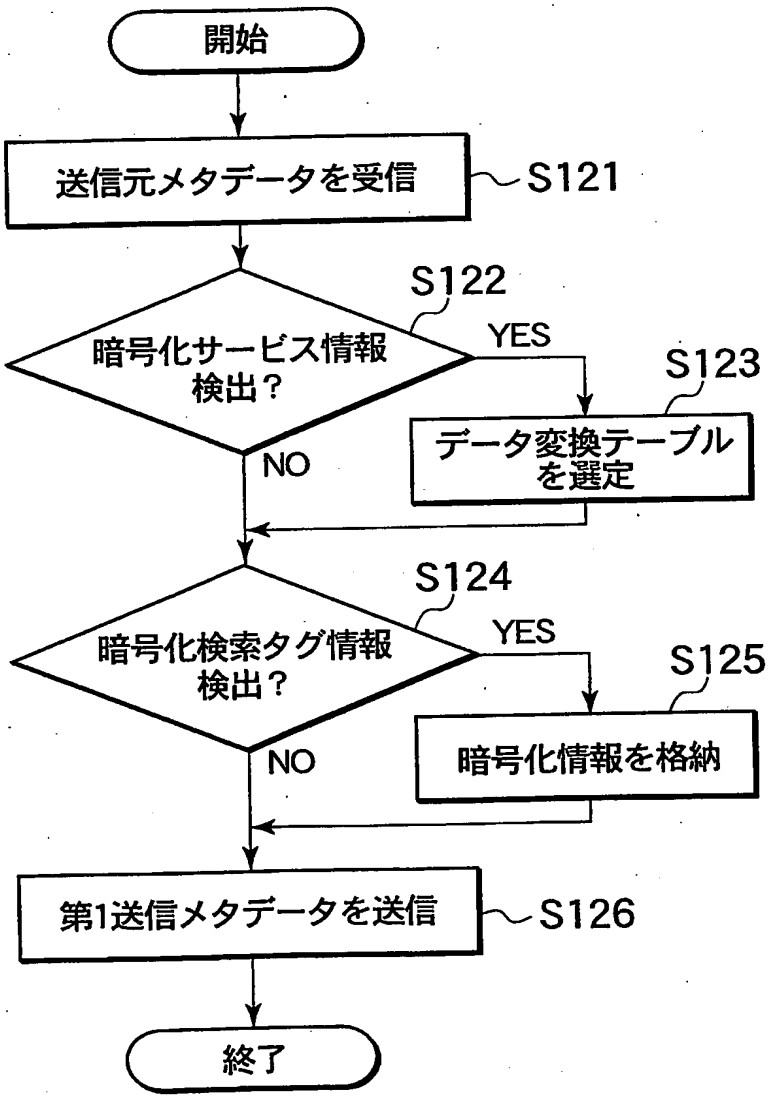

開始
送信元メタデータを受信
S121
S122
暗号化サービス情報検出？
YES
S123
データ変換テーブルを選定
NO
S124
暗号化検索タグ情報検出？
YES
S125
暗号化情報を格納
NO
第1送信メタデータを送信
S126
終了

FIG. 12

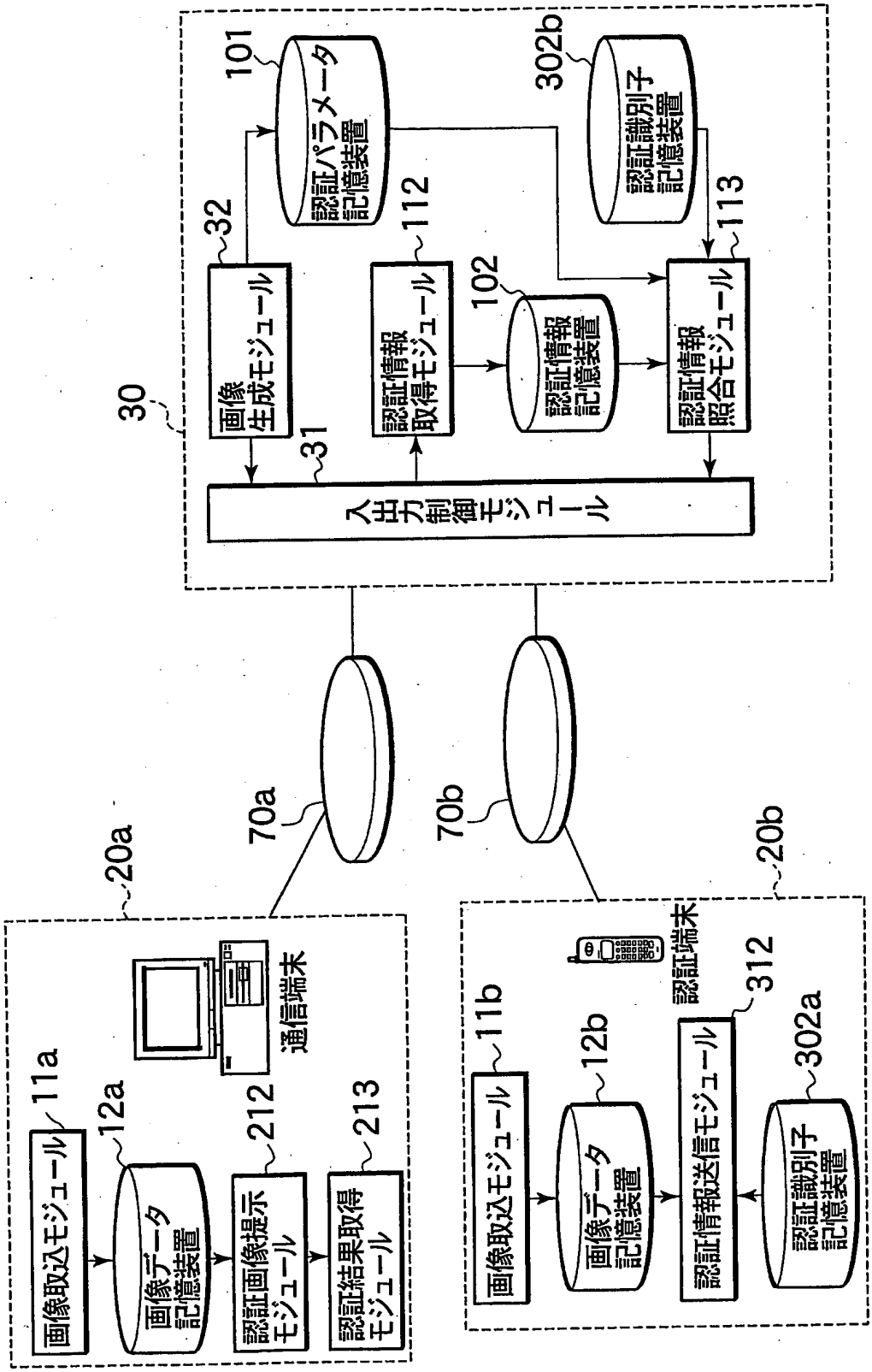

30
入出力制御モジュール
31
画像生成モジュール
32
認証パラメータ記憶装置
101
認証情報取得モジュール
112
認証情報記憶装置
102
認証情報照合モジュール
113
認証識別子記憶装置
302b
70a
70b
20a
画像取込モジュール
11a
画像データ記憶装置
12a
認証画像提示モジュール
212
認証結果取得モジュール
213
通信端末
20b
画像取込モジュール
11b
画像データ記憶装置
12b
認証情報送信モジュール
312
認証識別子記憶装置
302a
認証端末

FIG. 13

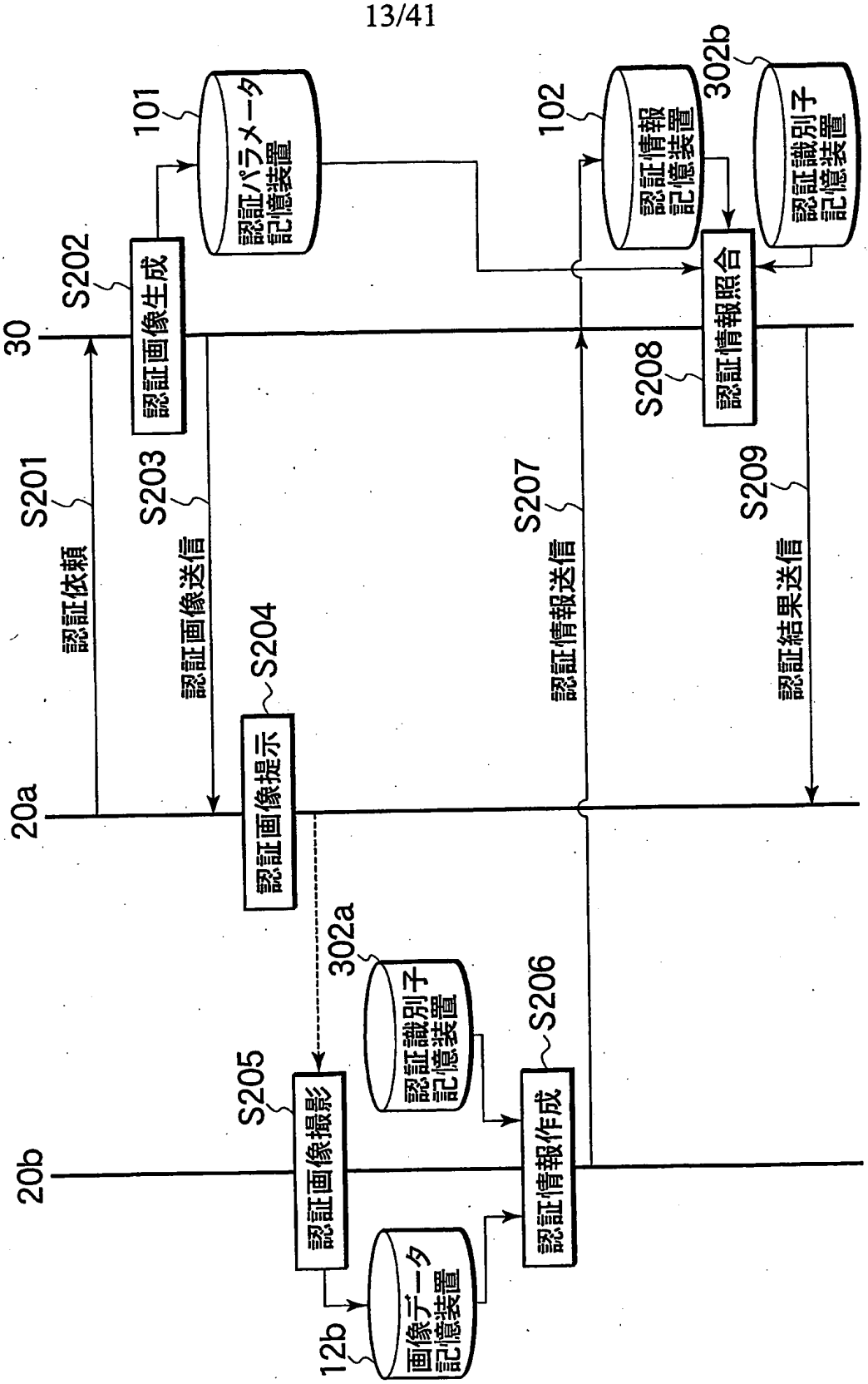

30
20a
20b
12b
S201
認証依頼
S202
認証画像生成
S203
認証画像送信
S204
認証画像提示
S205
認証画像撮影
S206
認証情報作成
S207
認証情報送信
S208
認証情報照合
S209
認証結果送信
101
認証パラメータ記憶装置
102
認証情報記憶装置
302a
認証識別子記憶装置
302b
認証識別子記憶装置
画像データ記憶装置

FIG. 14

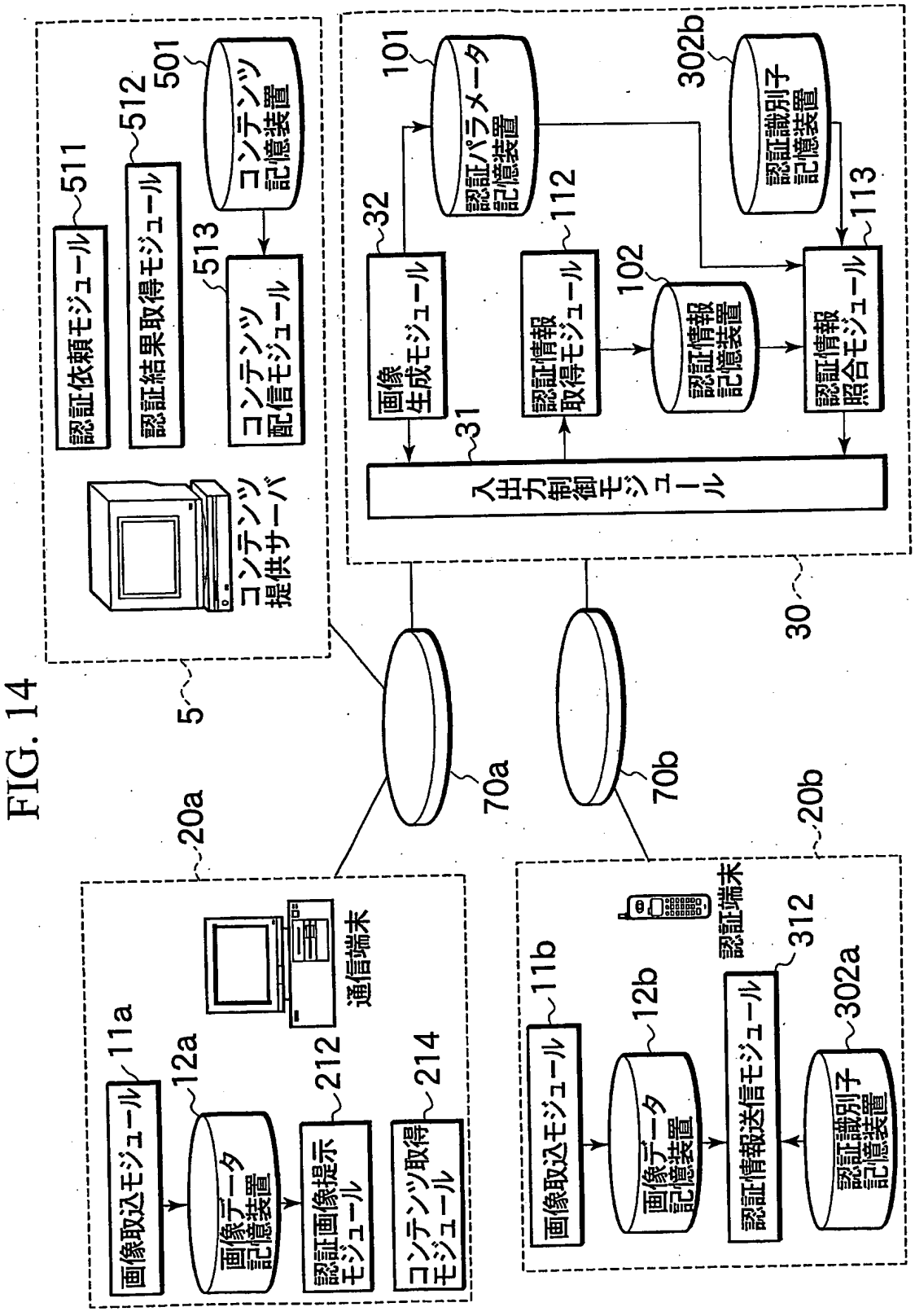

5
コンテンツ提供サーバ
認証依頼モジュール
511
認証結果取得モジュール
512
コンテンツ配信モジュール
513
コンテンツ記憶装置
501
30
入出力制御モジュール
画像生成モジュール
32
認証情報取得モジュール
112
認証情報照合モジュール
113
31
認証パラメータ記憶装置
101
認証情報記憶装置
102
認証識別子記憶装置
302b
70a
70b
20a
画像取込モジュール
11a
画像データ記憶装置
12a
認証画像提示モジュール
212
コンテンツ取得モジュール
214
通信端末
20b
画像取込モジュール
11b
画像データ記憶装置
12b
認証情報送信モジュール
312
認証識別子記憶装置
302a
認証端末

FIG. 15

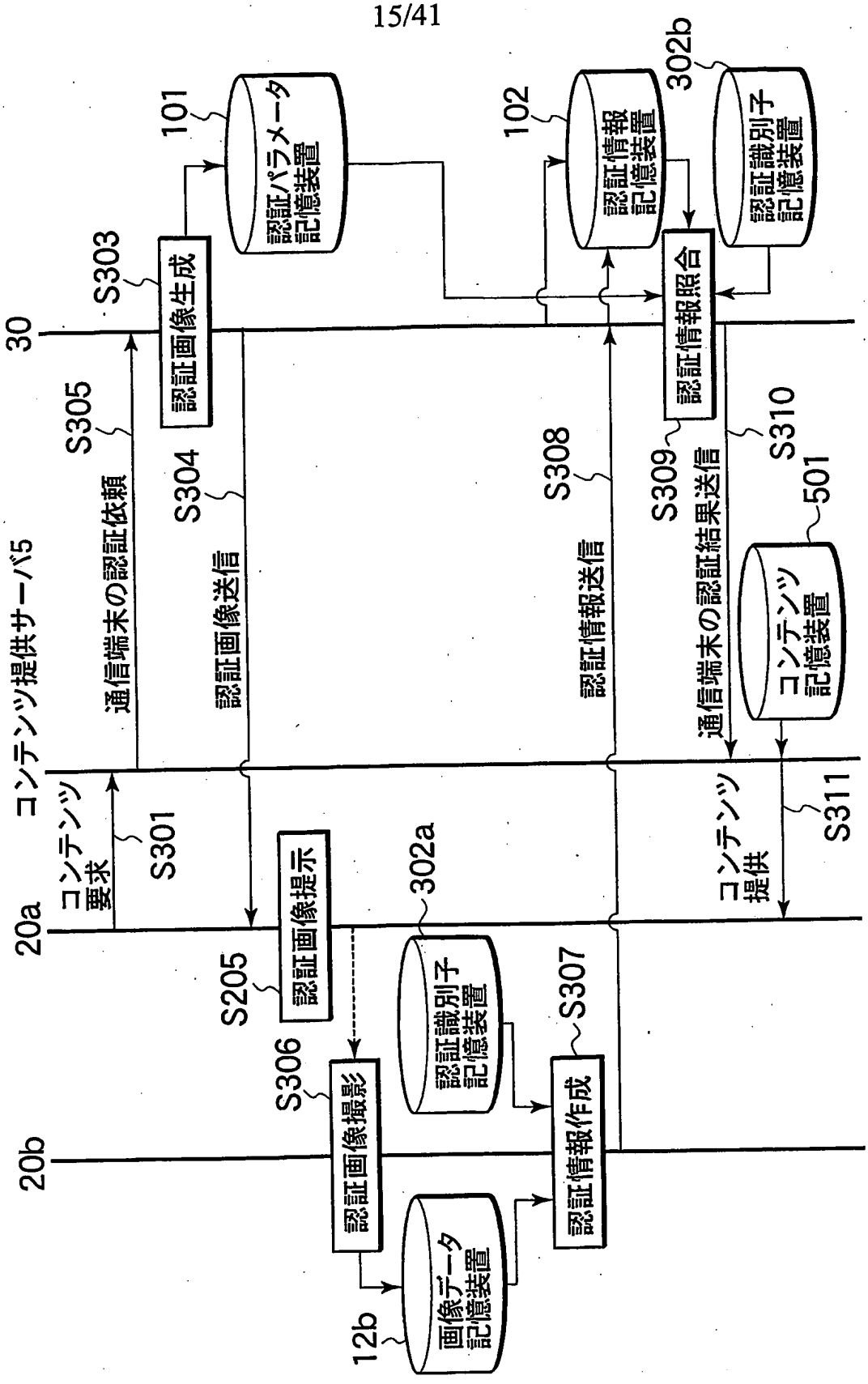

コンテンツ提供サーバ5
30
20a
20b
12b
101
認証パラメータ記憶装置
102
認証情報記憶装置
302b
認証識別子記憶装置
302a
認証識別子記憶装置
501
コンテンツ記憶装置
S303
認証画像生成
S305
通信端末の認証依頼
S304
認証画像送信
S308
認証情報送信
S309
認証情報照合
S310
通信端末の認証結果送信
S301
コンテンツ要求
S205
認証画像提示
S306
認証画像撮影
S307
認証情報作成
コンテンツ提供
S311
画像データ記憶装置

FIG. 16

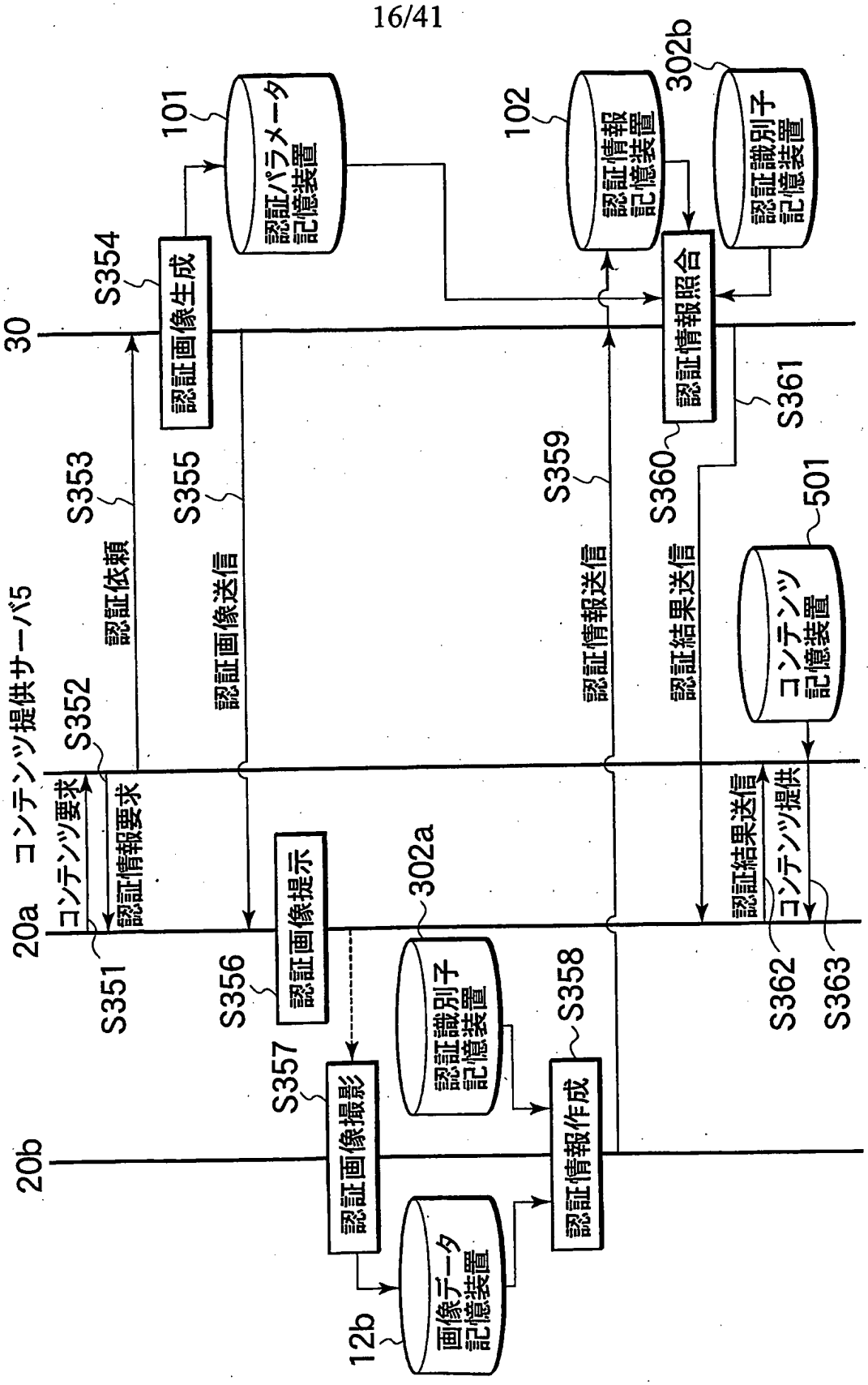

コンテンツ提供サーバ5
20a
20b
30
コンテンツ要求
認証情報要求
認証依頼
認証画像送信
認証画像提示
認証画像撮影
認証画像生成
認証情報送信
認証情報照合
認証結果送信
コンテンツ提供
認証結果送信
認証情報作成
S351
S352
S353
S354
S355
S356
S357
S358
S359
S360
S361
S362
S363
101
認証パラメータ記憶装置
102
認証情報記憶装置
302a
認証識別子記憶装置
302b
認証識別子記憶装置
501
コンテンツ記憶装置
12b
画像データ記憶装置

FIG. 17

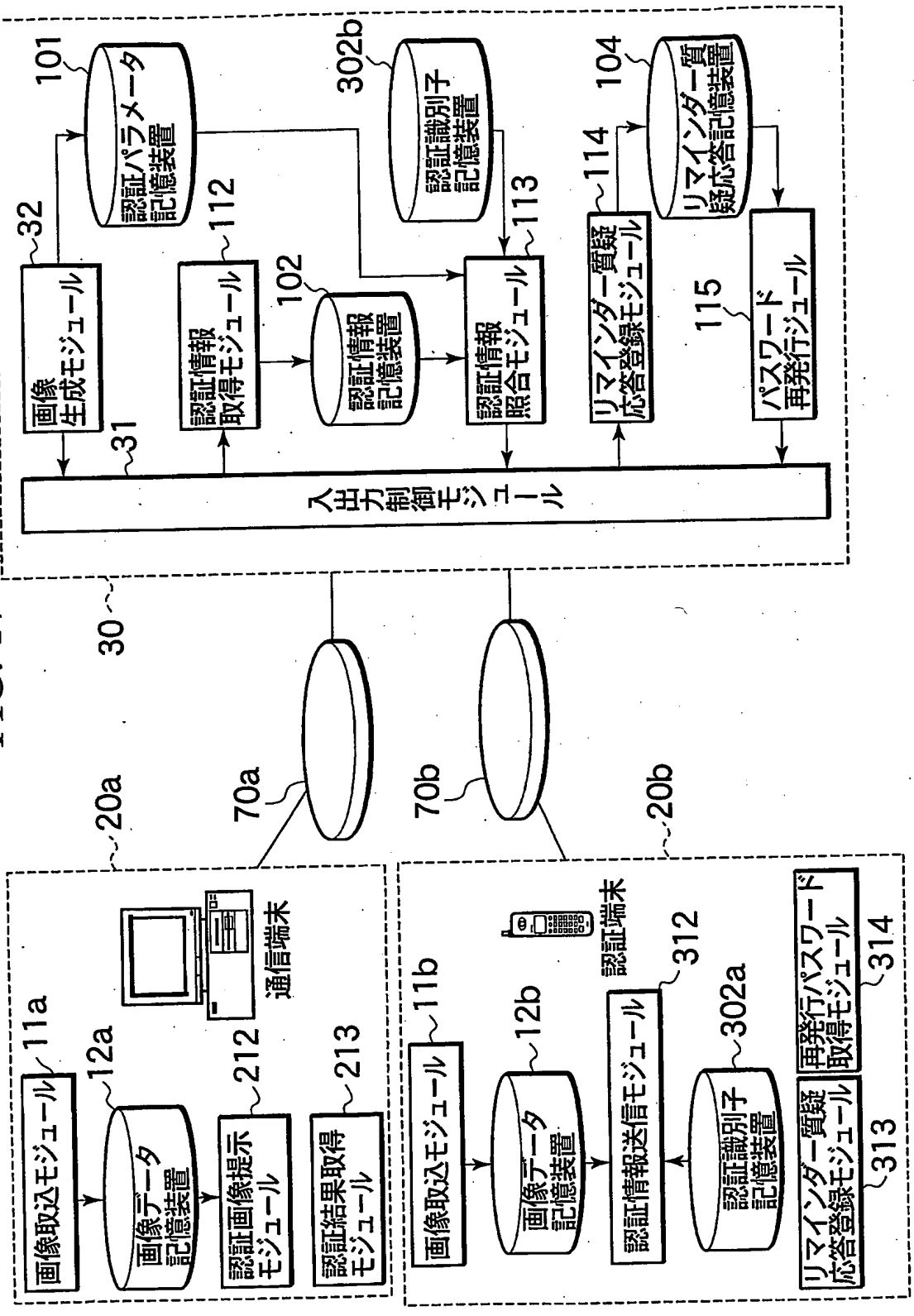

30
入出力制御モジュール
31
画像生成モジュール
32
認証パラメータ記憶装置
101
認証情報取得モジュール
112
認証情報記憶装置
102
認証識別子記憶装置
302b
認証情報照合モジュール
113
リマインダー質疑応答登録モジュール
114
リマインダー質疑応答記憶装置
104
パスワード再発行モジュール
115
70a
70b
20a
20b
画像取込モジュール
11a
画像データ記憶装置
12a
認証画像提示モジュール
212
認証結果取得モジュール
213
通信端末
画像取込モジュール
11b
画像データ記憶装置
12b
認証情報送信モジュール
312
認証識別子記憶装置
302a
リマインダー質疑応答登録モジュール
313
再発行パスワード取得モジュール
314
認証端末

FIG. 18

	候補	ジャンル	セレクトリスト	セレクト数
1	お母さんは何日生まれ？	家族	1~31日	31
2	お父さんは何日生まれ？	家族	1~31日	31
3	母親（父親）の旧姓の頭文字は？	家族	あ・か・が・さ・ざ・た・だ・な・は・ば・ぱ・ま・や・ら・わ行	15
4	あなたの生まれた市区町村の頭文字	思い出・心	あ・か・が・さ・ざ・た・だ・な・は・ば・ぱ・ま・や・ら・わ行	15
5	初恋の人の苗字の頭文字は？	思い出・心	あ・か・が・さ・ざ・た・だ・な・は・ば・ぱ・ま・や・ら・わ行	15
6	最初に飼ったペットの名前の頭文字	思い出・心	あ・か・が・さ・ざ・た・だ・な・は・ば・ぱ・ま・や・ら・わ行	15
7	初めて観た映画のタイトルの頭文字	思い出・心	あ・か・が・さ・ざ・た・だ・な・は・ば・ぱ・ま・や・ら・わ行	15
8	尊敬する人の苗字の頭文字は？	思い出・心	あ・か・が・さ・ざ・た・だ・な・は・ば・ぱ・ま・や・ら・わ行	15
9	母方の祖父の下の名前の頭文字は？	家族	あ・か・が・さ・ざ・た・だ・な・は・ば・ぱ・ま・や・ら・わ行	15
10	いとこは何人いる？	家族	0~14、15以上	16
11	初めての担任の先生の苗字の頭文字	思い出・心	あ・か・が・さ・ざ・た・だ・な・は・ば・ぱ・ま・や・ら・わ行	15

FIG. 19

英：A-Z、数：0-9	
4桁（英数）	1,679,616
5桁（英数）	60,466,176
6桁（英数）	2,176,782,336
7桁（英数）	78,364,164,096
8桁（英数）	2,821,109,907,456
4桁（数）	10,000
5桁（数）	100,000
6桁（数）	1000,000
7桁（数）	10,000,000
8桁（数）	100,000,000

FIG. 20

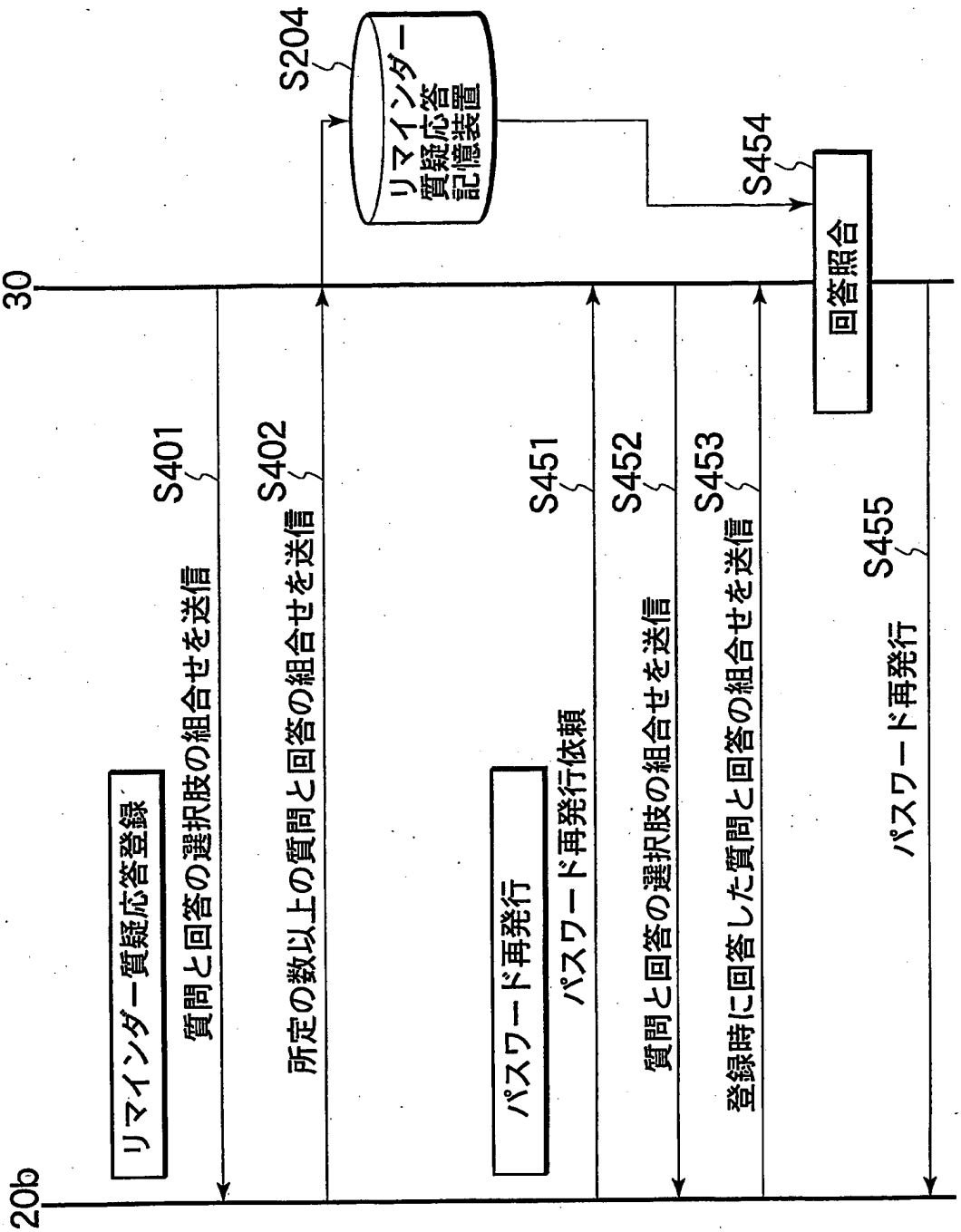

S204
リマインダー
質疑応答
記憶装置
S454
30
回答照合
S401
S402
S451
S452
S453
S455
リマインダー質疑応答登録
質問と回答の選択肢の組合せを送信
所定の数以上の質問と回答の組合せを送信
パスワード再発行
パスワード再発行依頼
質問と回答の選択肢の組合せを送信
登録時に回答した質問と回答の組合せを送信
パスワード再発行
20b

FIG. 21

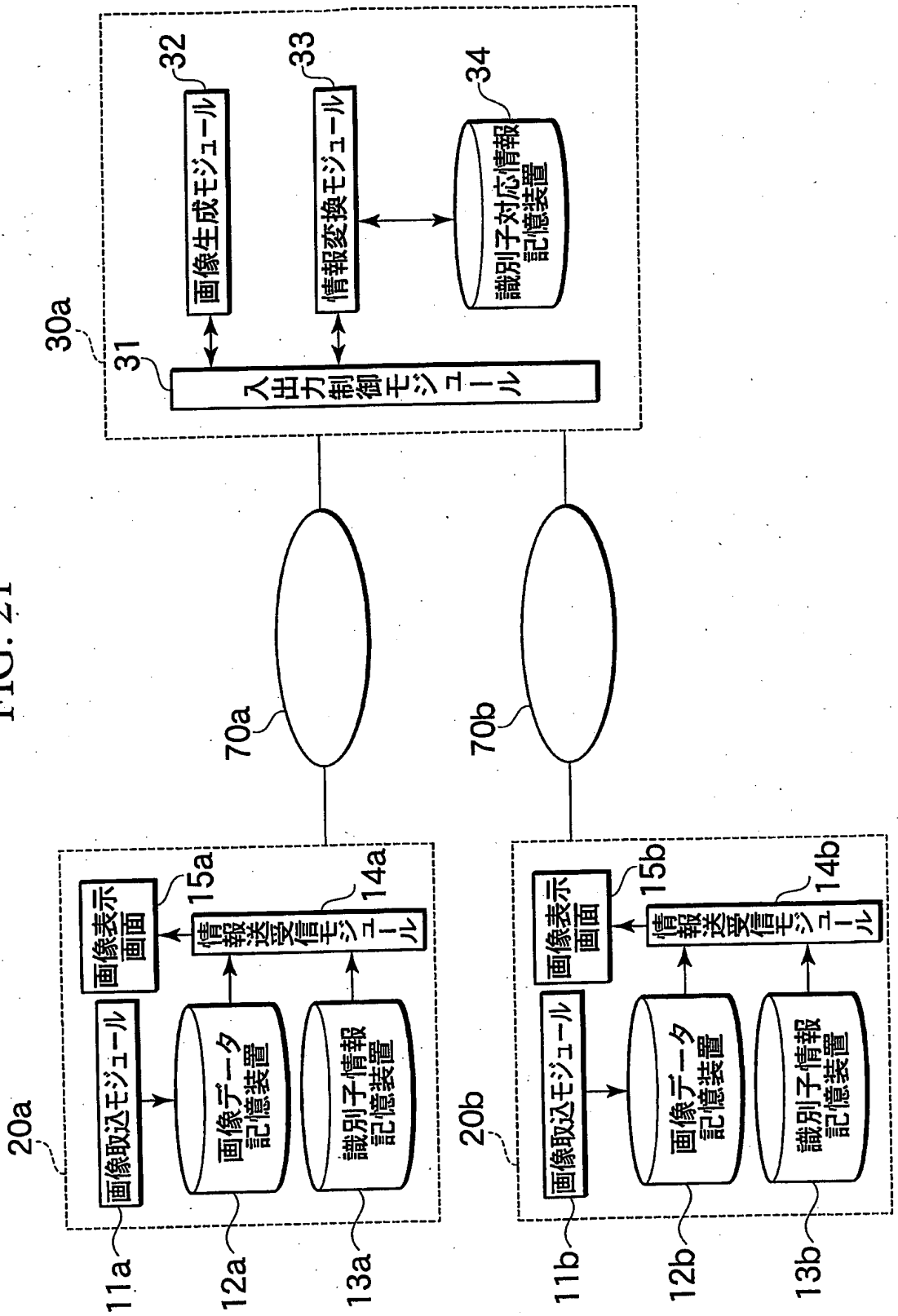

30a
31
入出力制御モジュール
32
画像生成モジュール
33
情報変換モジュール
34
識別子対応情報記憶装置
70a
70b
20a
画像取込モジュール
画像データ記憶装置
識別子情報記憶装置
情報送受信モジュール
画像表示画面
15a
14a
11a
12a
13a
20b
画像取込モジュール
画像データ記憶装置
識別子情報記憶装置
情報送受信モジュール
画像表示画面
15b
14b
11b
12b
13b

FIG. 22

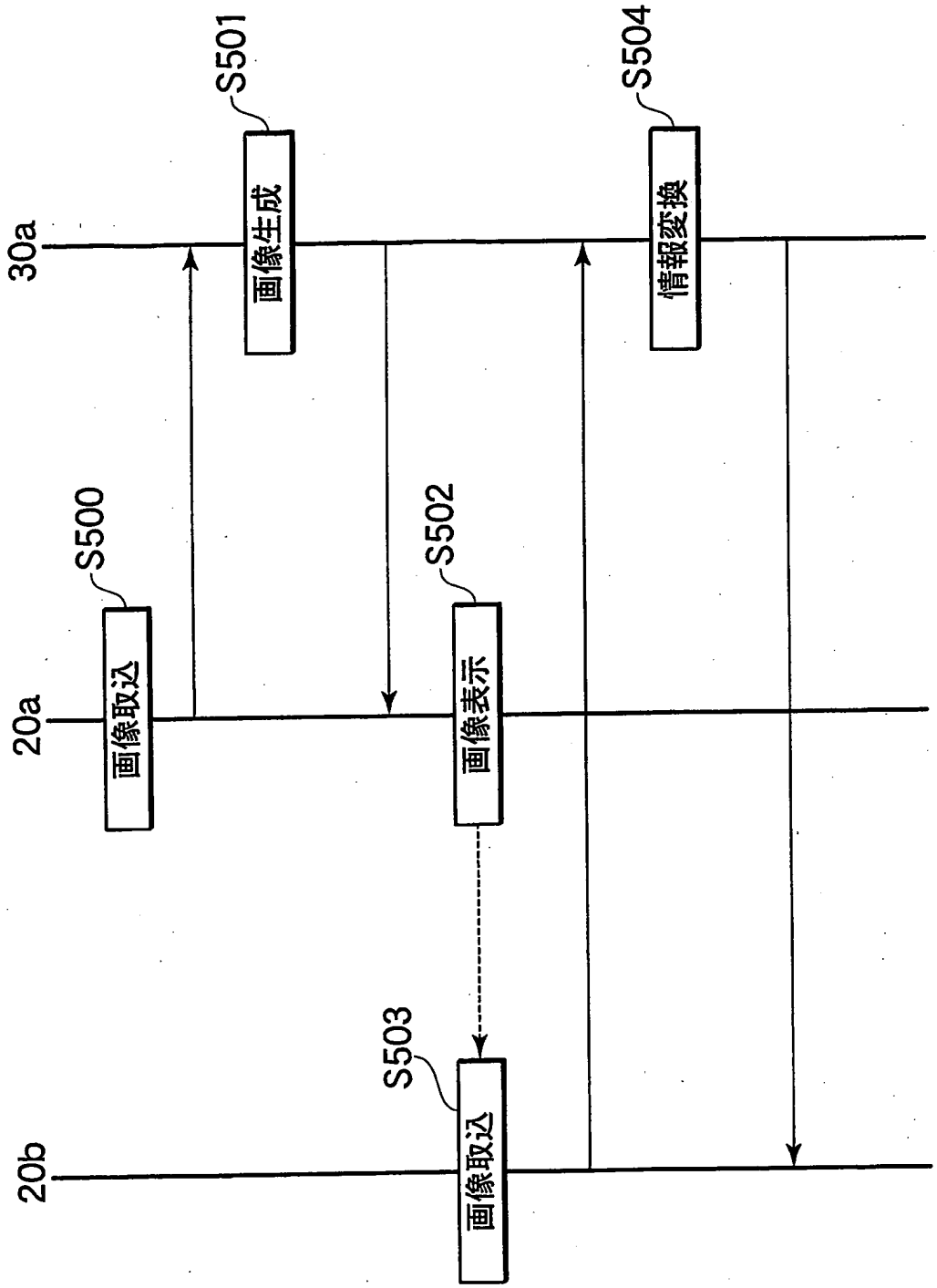


FIG. 23

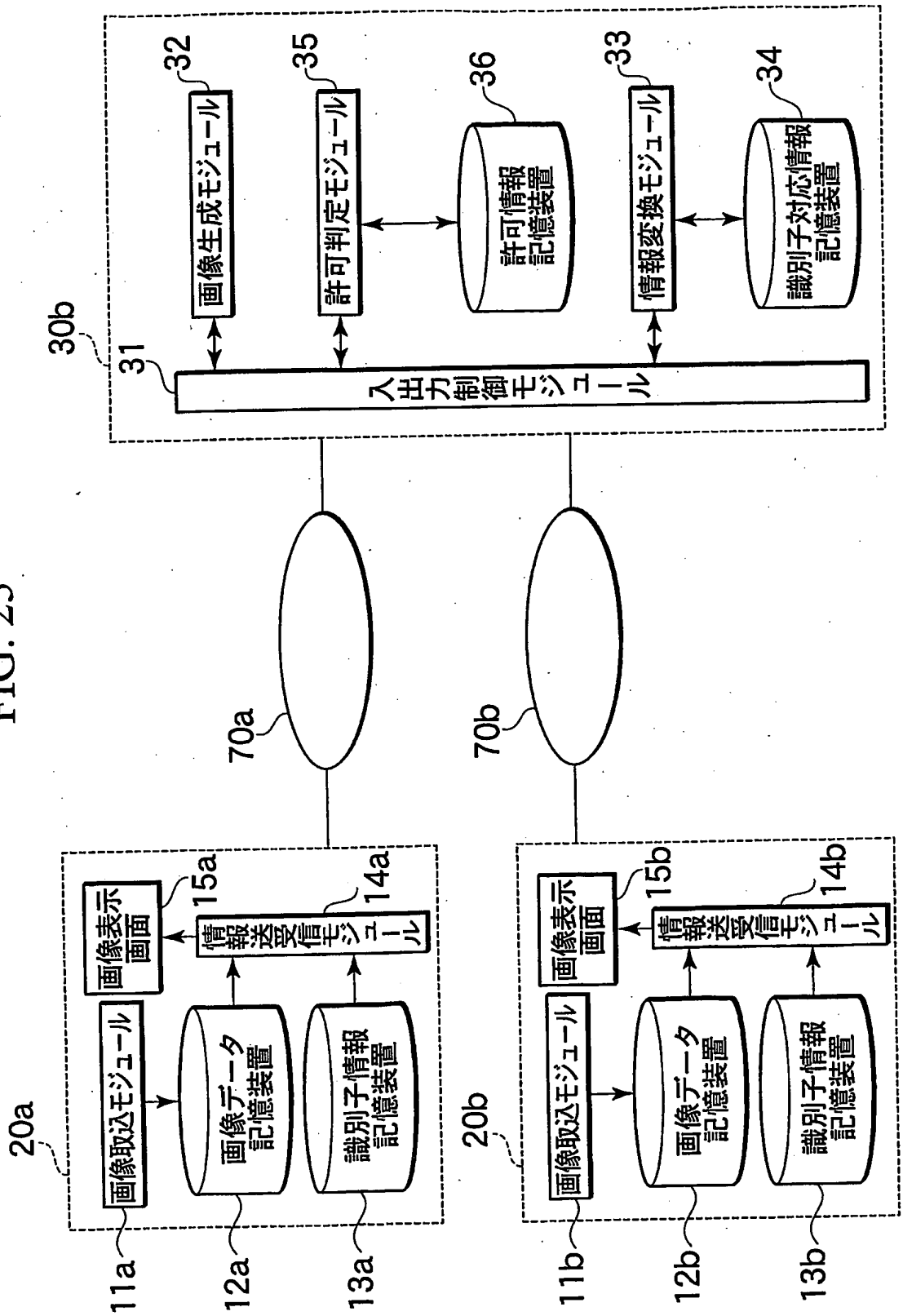

30b
31
入出力制御モジュール
32
画像生成モジュール
35
許可判定モジュール
36
許可情報記憶装置
33
情報変換モジュール
34
識別子対応情報記憶装置
70a
70b
20a
画像取込モジュール
画像データ記憶装置
識別子情報記憶装置
情報送受信モジュール
画像表示画面
15a
14a
11a
12a
13a
20b
画像取込モジュール
画像データ記憶装置
識別子情報記憶装置
情報送受信モジュール
画像表示画面
15b
14b
11b
12b
13b

FIG. 24

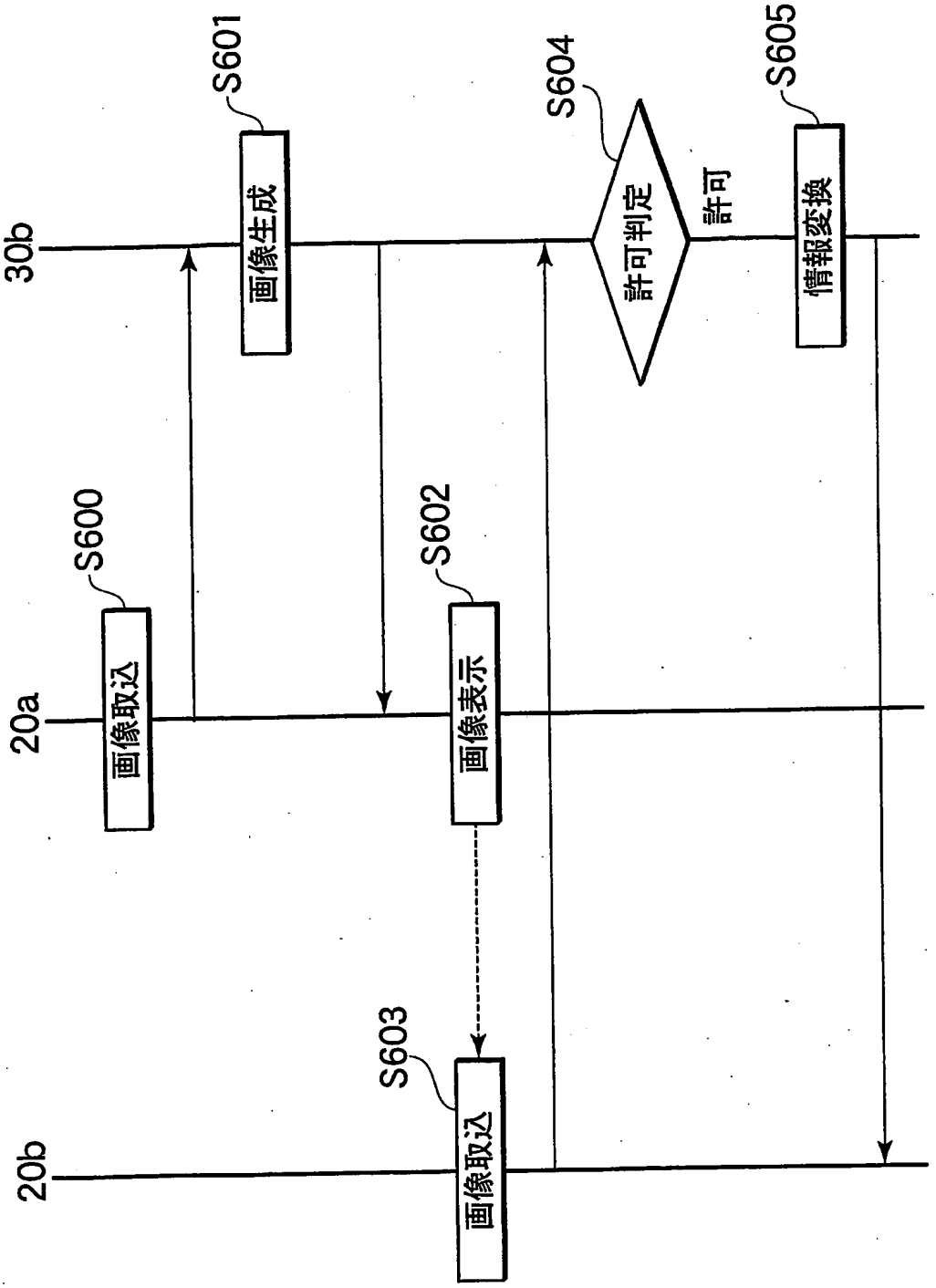

30b
20a
20b
S600
S601
S602
S603
S604
S605
画像取込
画像生成
画像表示
画像取込
許可判定
許可
情報変換

FIG. 25

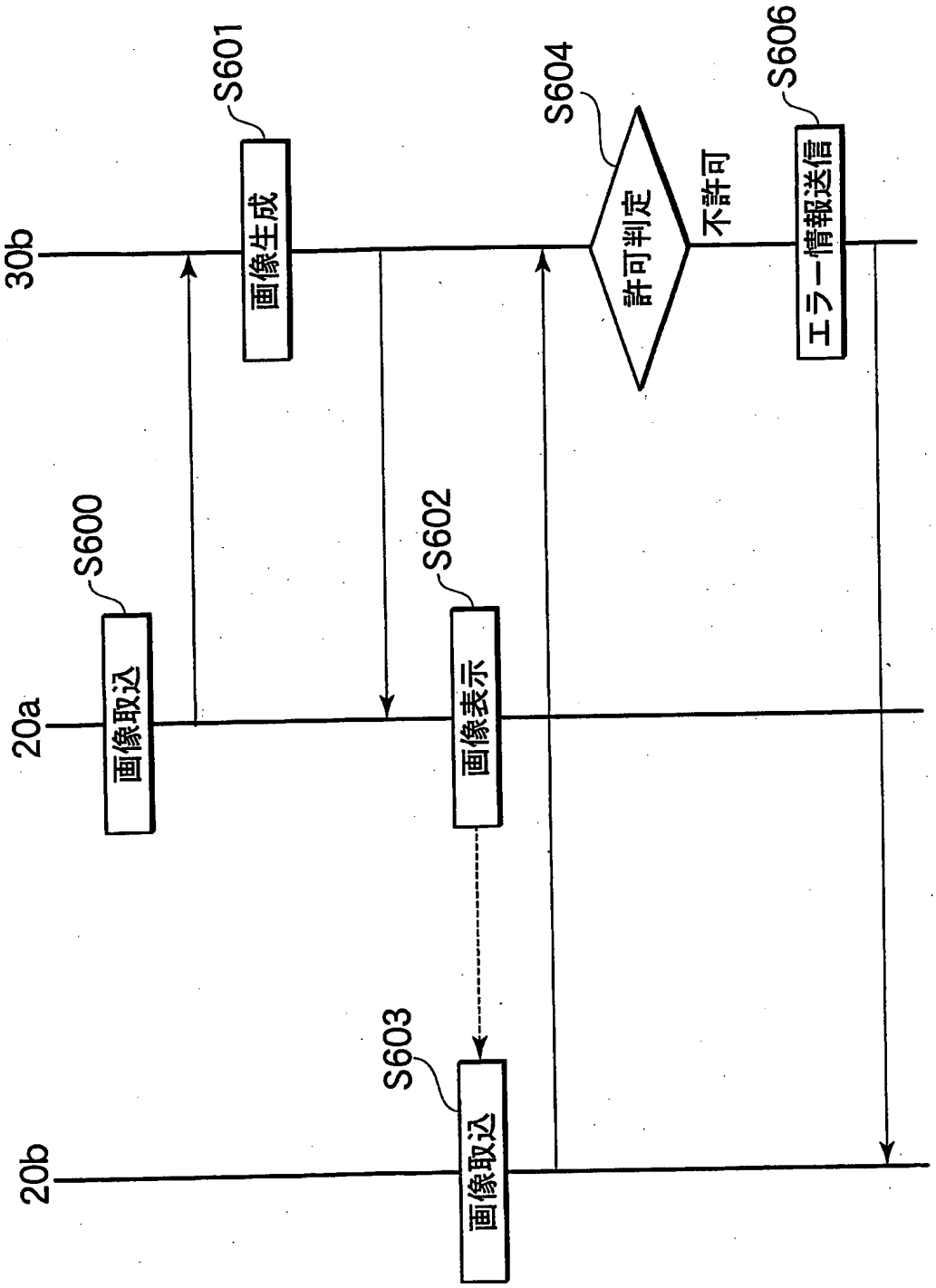

S601
S604
S606
30b
画像生成
許可判定
不許可
エラー情報送信
S600
S602
20a
画像取込
画像表示
S603
20b
画像取込

FIG. 26

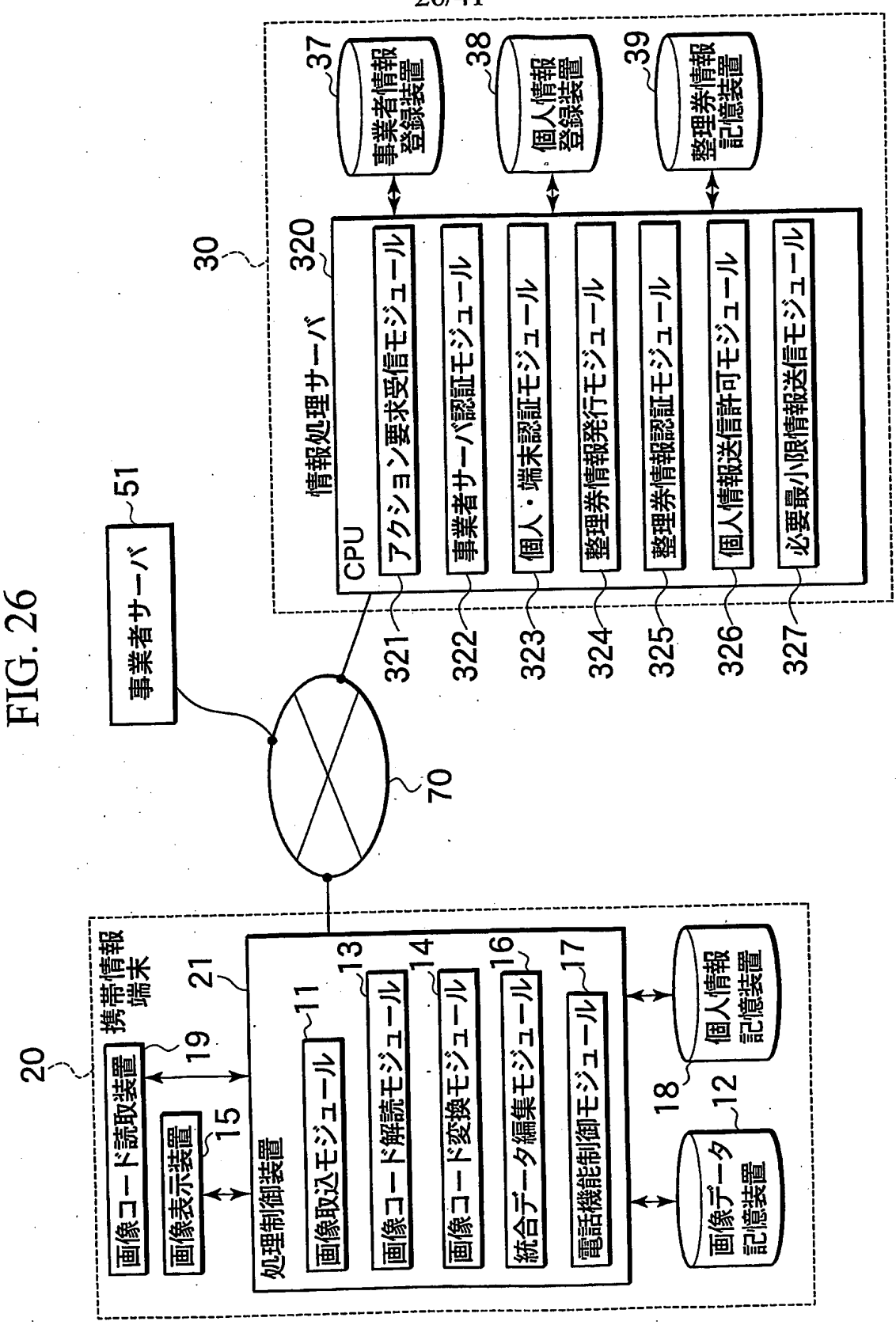

20
携帯情報端末
画像コード読取装置
画像表示装置
19
15
処理制御装置
21
画像取込モジュール
11
画像コード解読モジュール
13
画像コード変換モジュール
14
統合データ編集モジュール
16
電話機能制御モジュール
17
18
個人情報記憶装置
12
画像データ記憶装置
70
事業者サーバ
51
30
情報処理サーバ
320
CPU
アクション要求受信モジュール
321
事業者サーバ認証モジュール
322
個人・端末認証モジュール
323
整理券情報発行モジュール
324
整理券情報認証モジュール
325
個人情報送信許可モジュール
326
必要最小限情報送信モジュール
327
37
事業者情報登録装置
38
個人情報登録装置
39
整理券情報記憶装置

FIG. 27

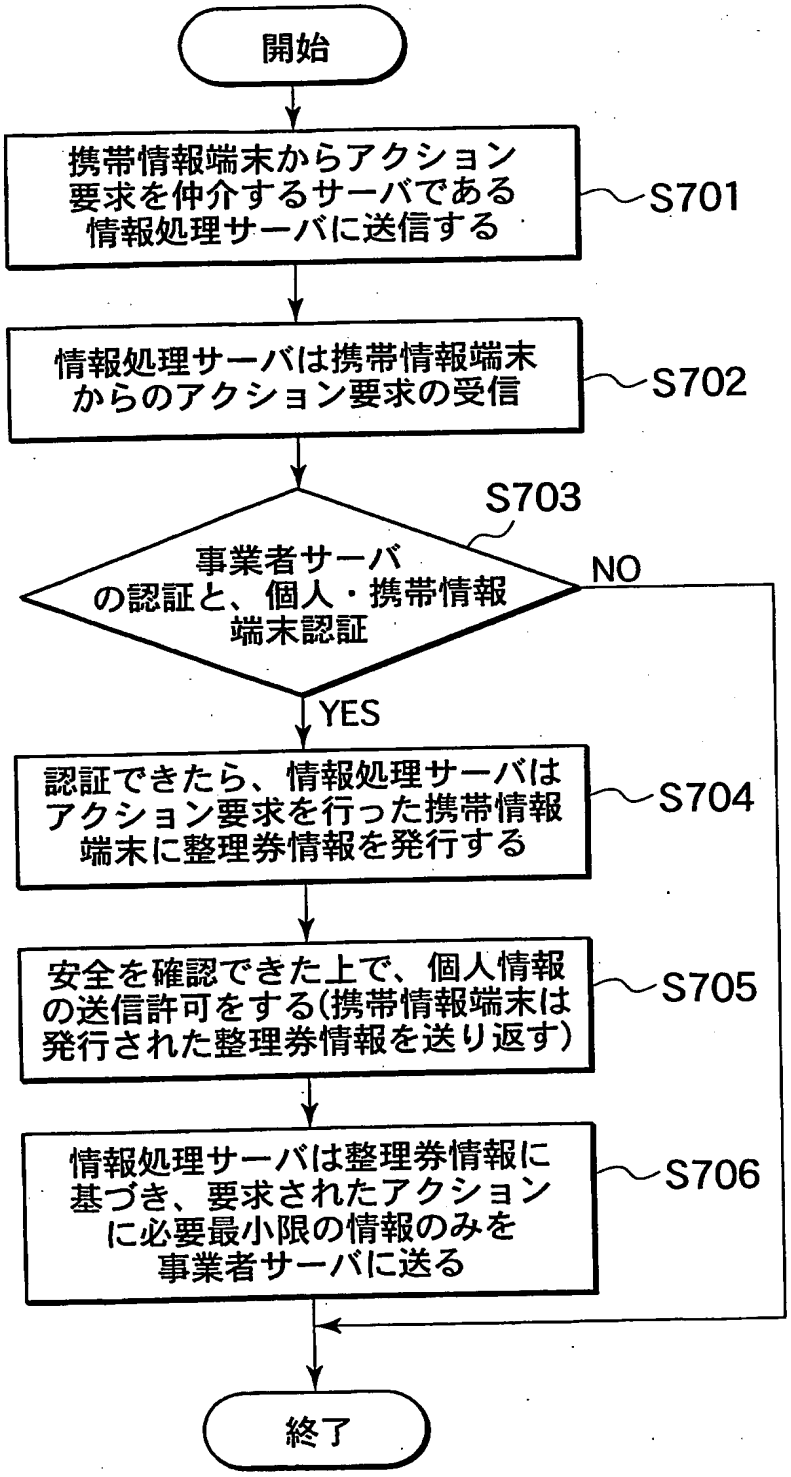

開始
携帯情報端末からアクション要求を仲介するサーバである情報処理サーバに送信する
S701
情報処理サーバは携帯情報端末からのアクション要求の受信
S702
S703
事業者サーバの認証と、個人・携帯情報端末認証
NO
YES
認証できたら、情報処理サーバはアクション要求を行った携帯情報端末に整理券情報を発行する
S704
安全を確認できた上で、個人情報の送信許可をする(携帯情報端末は発行された整理券情報を送り返す)
S705
情報処理サーバは整理券情報に基づき、要求されたアクションに必要最小限の情報のみを事業者サーバに送る
S706
終了

FIG. 28

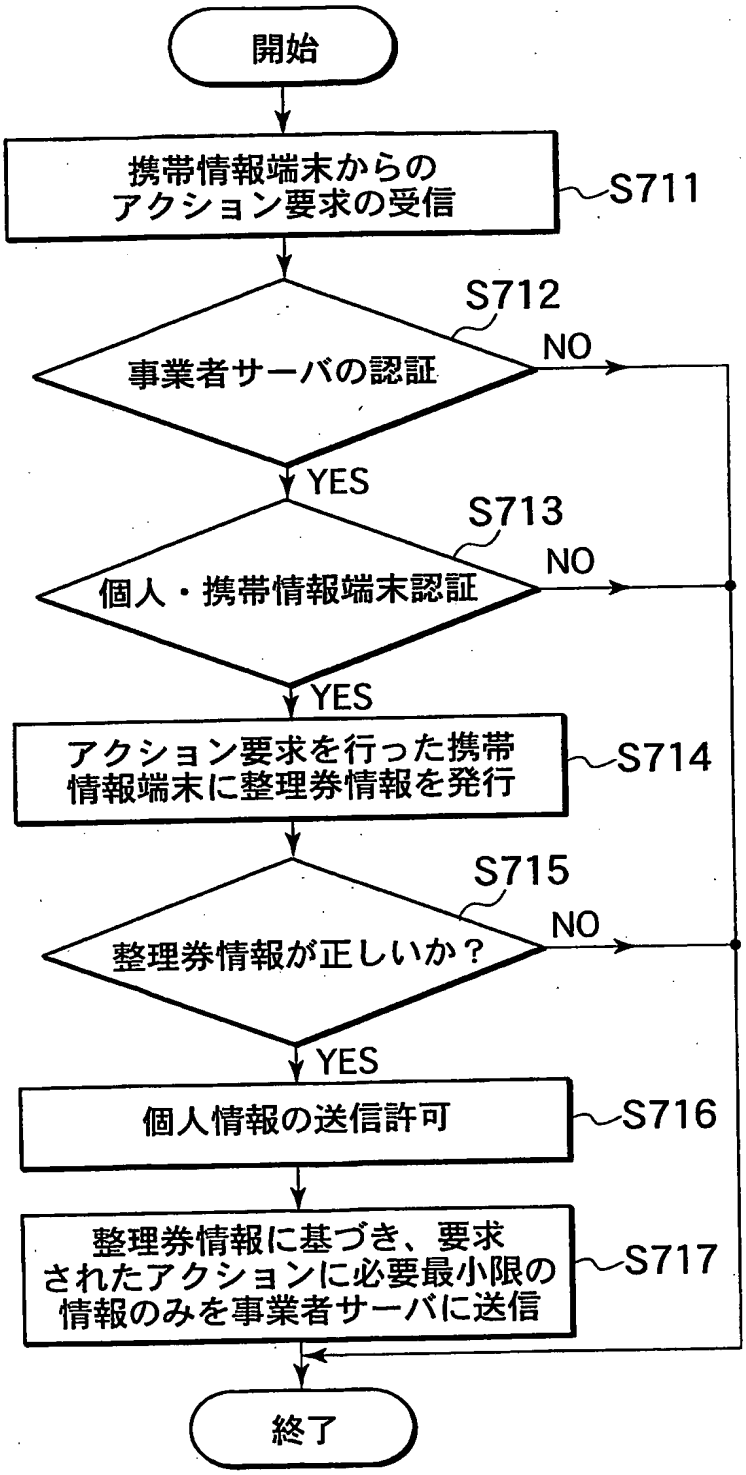

開始
携帯情報端末からのアクション要求の受信
S711
S712
事業者サーバの認証
NO
YES
S713
個人・携帯情報端末認証
NO
YES
アクション要求を行った携帯情報端末に整理券情報を発行
S714
S715
整理券情報が正しいか？
NO
YES
個人情報の送信許可
S716
整理券情報に基づき、要求されたアクションに必要最小限の情報のみを事業者サーバに送信
S717
終了

FIG. 29

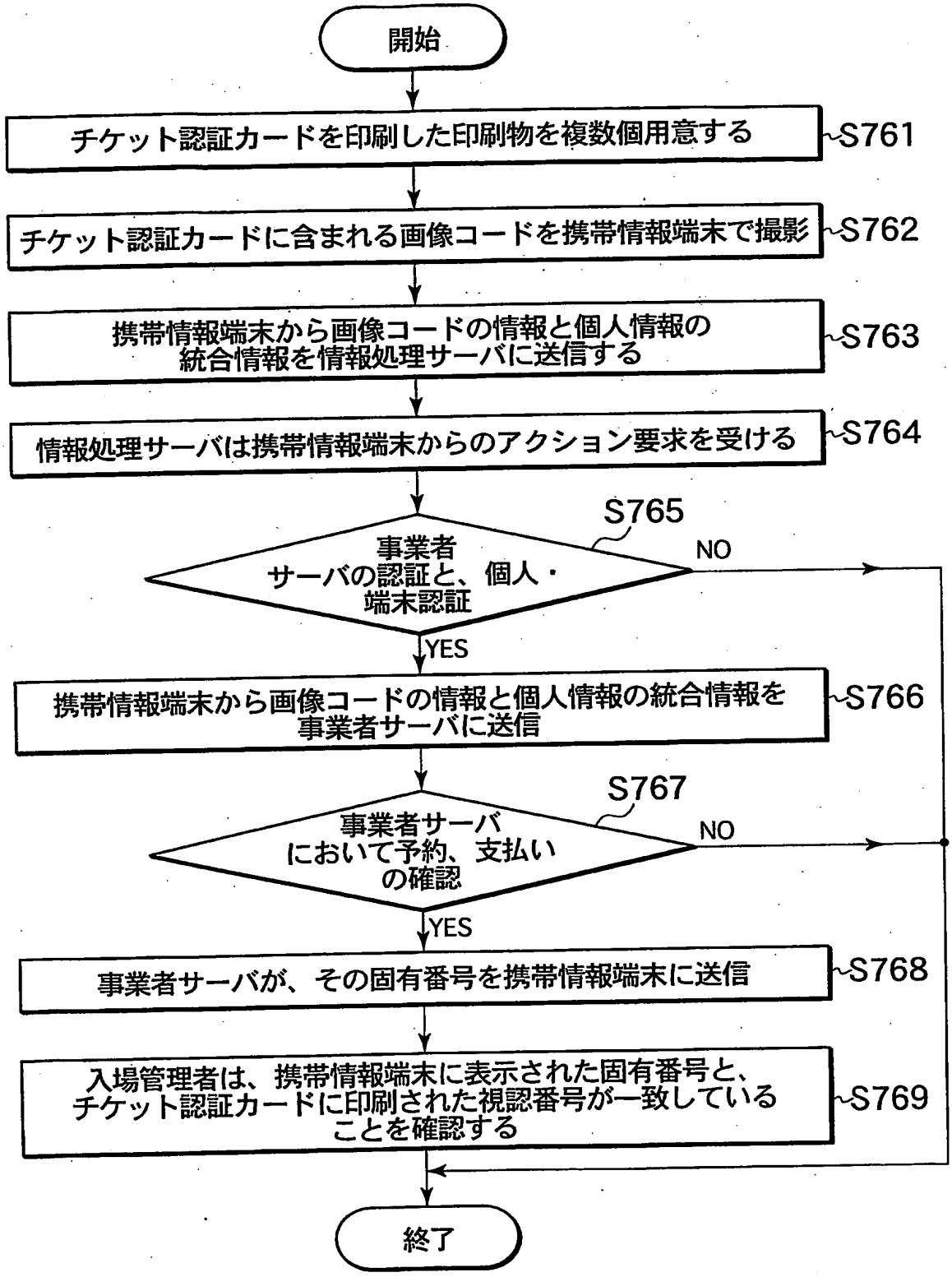

開始
チケット認証カードを印刷した印刷物を複数個用意する
S761
チケット認証カードに含まれる画像コードを携帯情報端末で撮影
S762
携帯情報端末から画像コードの情報と個人情報の統合情報を情報処理サーバに送信する
S763
情報処理サーバは携帯情報端末からのアクション要求を受ける
S764
S765
事業者サーバの認証と、個人・端末認証
NO
YES
携帯情報端末から画像コードの情報と個人情報の統合情報を事業者サーバに送信
S766
S767
事業者サーバにおいて予約、支払いの確認
NO
YES
事業者サーバが、その固有番号を携帯情報端末に送信
S768
入場管理者は、携帯情報端末に表示された固有番号と、チケット認証カードに印刷された視認番号が一致していることを確認する
S769
終了

FIG.30

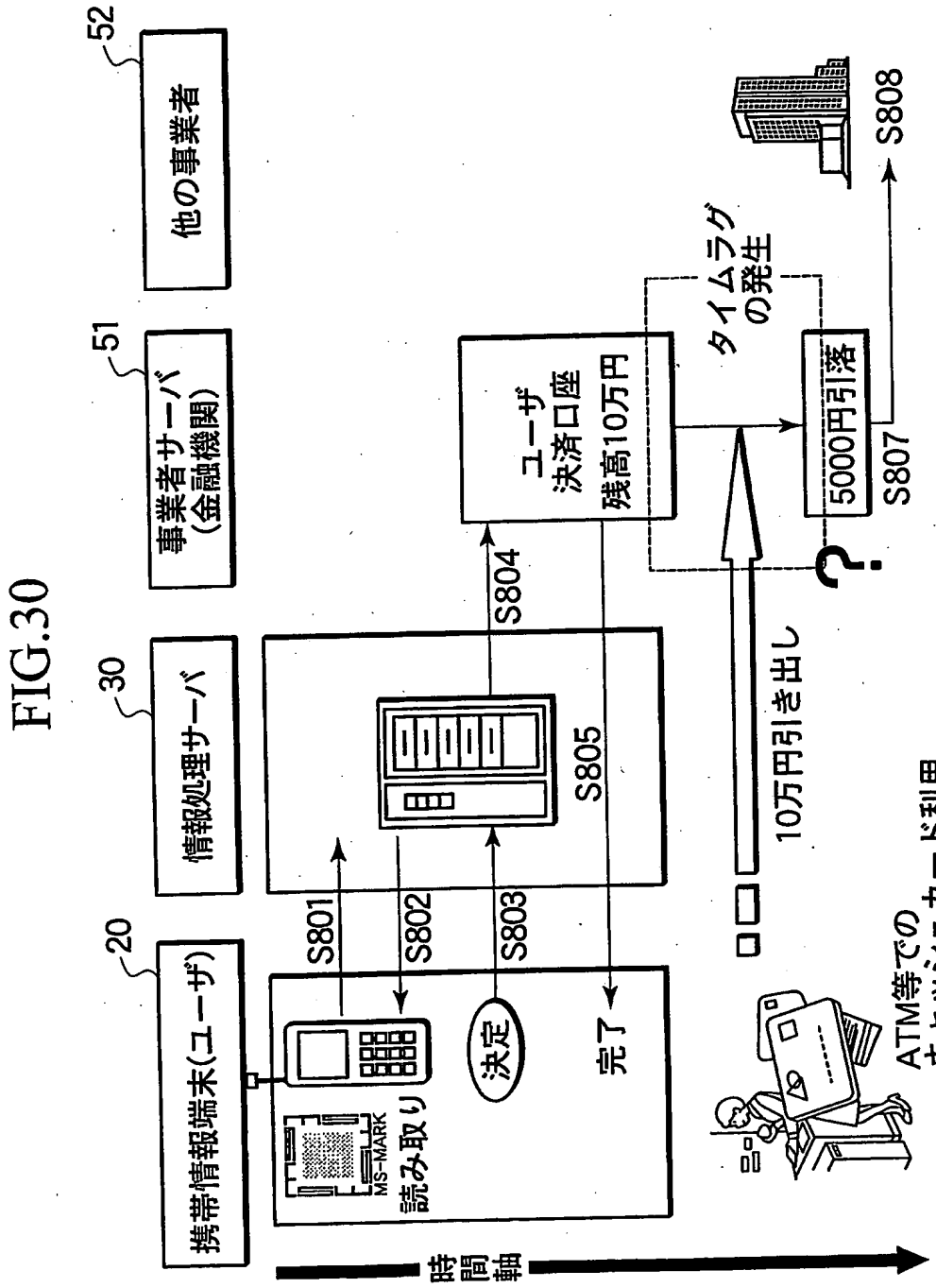

52
他の事業者
51
事業者サーバ
(金融機関)
30
情報処理サーバ
20
携帯情報端末(ユーザ)
S801
S802
S803
S804
S805
MS-MARK
読み取り
決定
完了
ユーザ
決済口座
残高10万円
タイムラグ
の発生
5000円引落
S807
S808
10万円引き出し
ATM等での
キャッシュカード利用
時間軸

FIG. 31

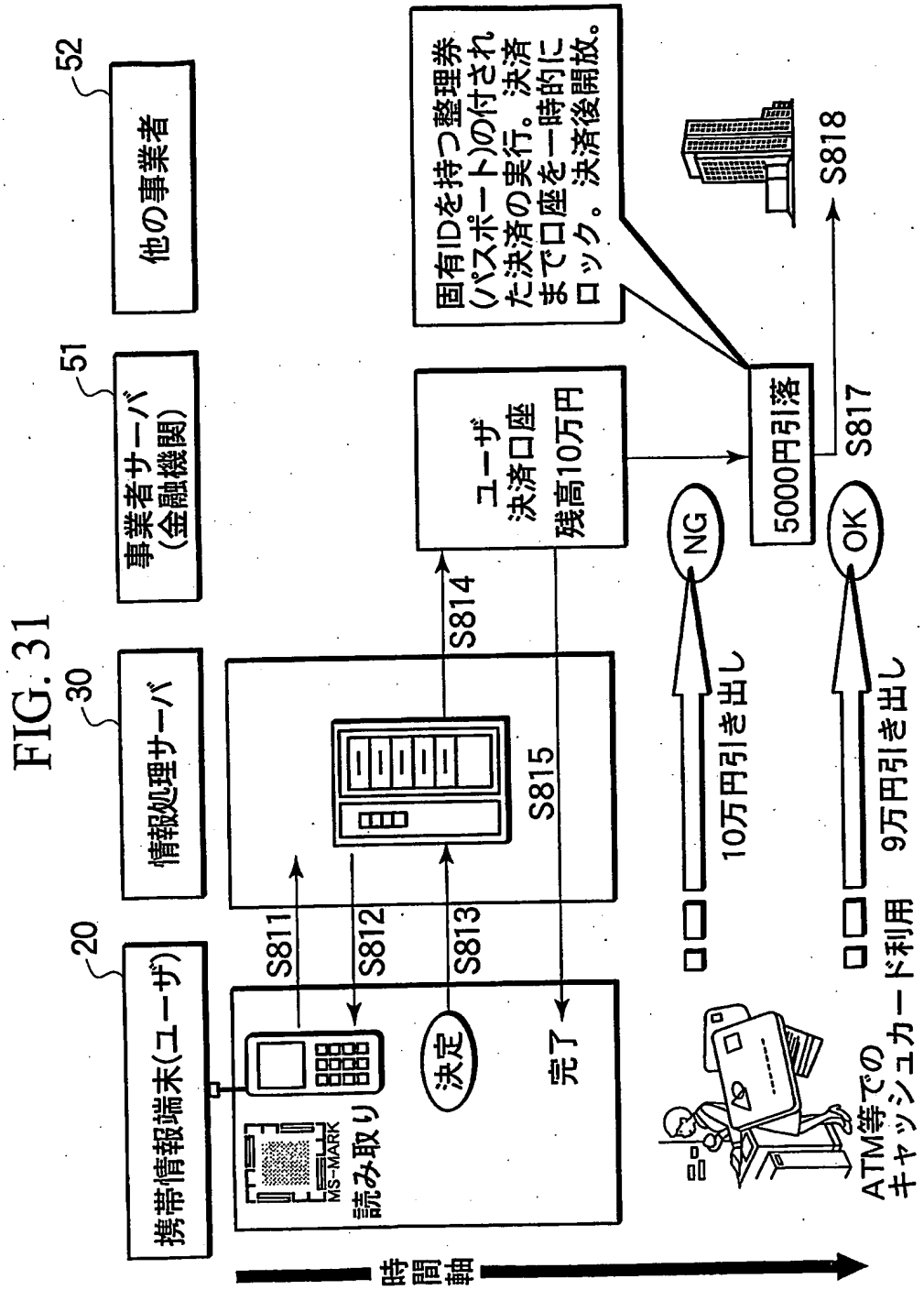

52
他の事業者
51
事業者サーバ
(金融機関)
30
情報処理サーバ
20
携帯情報端末(ユーザ)
固有IDを持つ整理券
(パスポート)の付され
た決済の実行。決済
まで口座を一時的に
ロック。決済後開放。
ユーザ
決済口座
残高10万円
5000円引落
S818
S817
S814
S815
S811
S812
S813
NG
OK
10万円引き出し
9万円引き出し
MS-MARK
読み取り
決定
完了
ATM等での
キャッシュカード利用
時間軸

FIG. 32

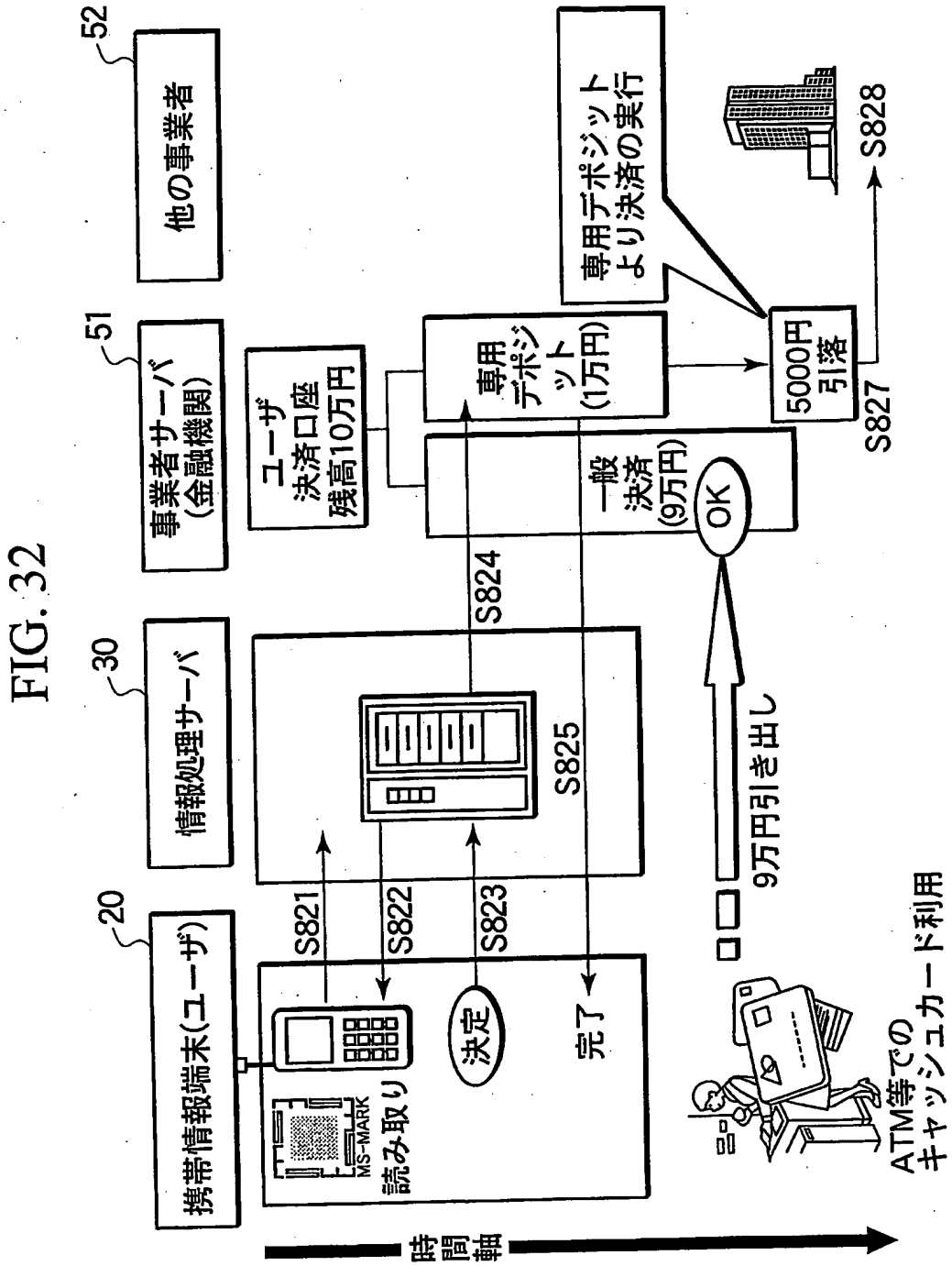

52
他の事業者
51
事業者サーバ
(金融機関)
ユーザ
決済口座
残高10万円
専用
デポジット
(1万円)
専用デポジット
より決済の実行
5000円
引落
S827
S828
30
情報処理サーバ
S824
一般
決済
(9万円)
OK
S825
20
携帯情報端末(ユーザ)
S821
S822
S823
MS-MARK
読み取り
決定
完了
9万円引き出し
ATM等での
キャッシュカード利用
時間軸

FIG. 33

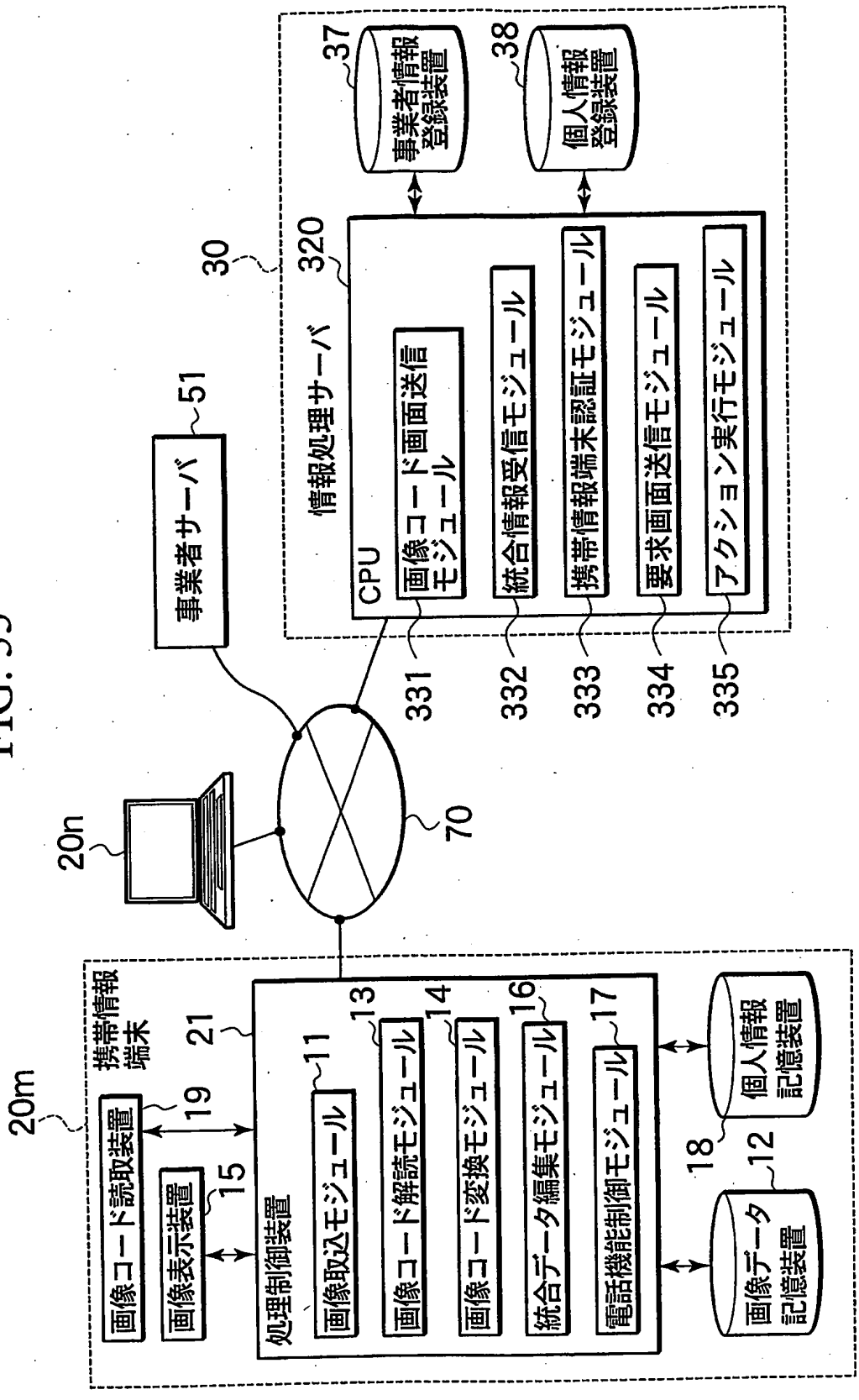

携帯情報端末
20m
画像コード読取装置
19
画像表示装置
15
処理制御装置
21
画像取込モジュール
11
画像コード解読モジュール
13
画像コード変換モジュール
14
統合データ編集モジュール
16
電話機能制御モジュール
17
18
個人情報記憶装置
画像データ記憶装置
12
20n
70
事業者サーバ
51
30
情報処理サーバ
320
CPU
画像コード画面送信モジュール
331
統合情報受信モジュール
332
携帯情報端末認証モジュール
333
要求画面送信モジュール
334
アクション実行モジュール
335
37
事業者情報登録装置
38
個人情報登録装置

FIG. 34

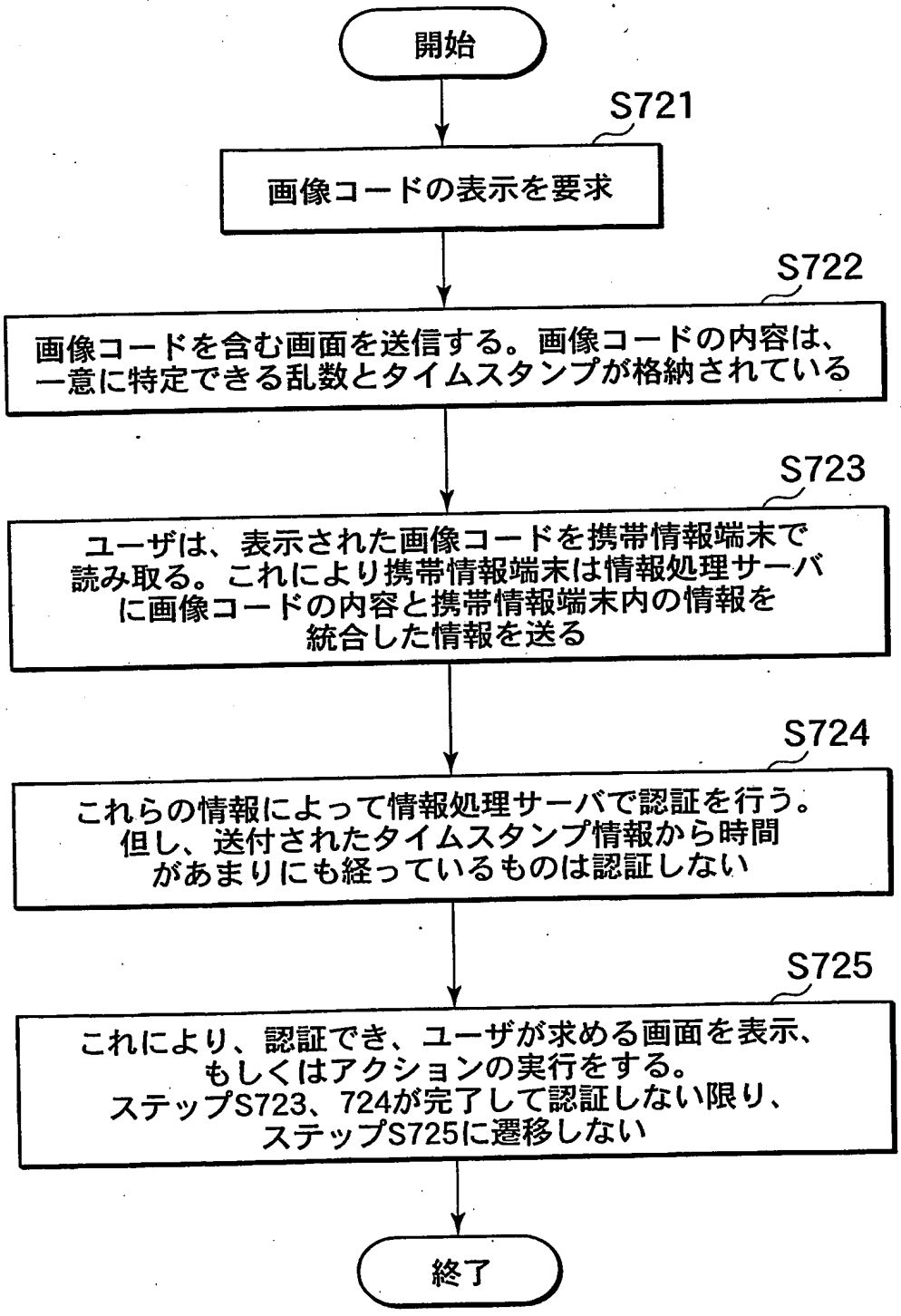

開始
S721
画像コードの表示を要求
S722
画像コードを含む画面を送信する。画像コードの内容は、一意に特定できる乱数とタイムスタンプが格納されている
S723
ユーザは、表示された画像コードを携帯情報端末で読み取る。これにより携帯情報端末は情報処理サーバに画像コードの内容と携帯情報端末内の情報を統合した情報を送る
S724
これらの情報によって情報処理サーバで認証を行う。但し、送付されたタイムスタンプ情報から時間があまりにも経っているものは認証しない
S725
これにより、認証でき、ユーザが求める画面を表示、もしくはアクションの実行をする。ステップS723、724が完了して認証しない限り、ステップS725に遷移しない
終了

FIG. 35

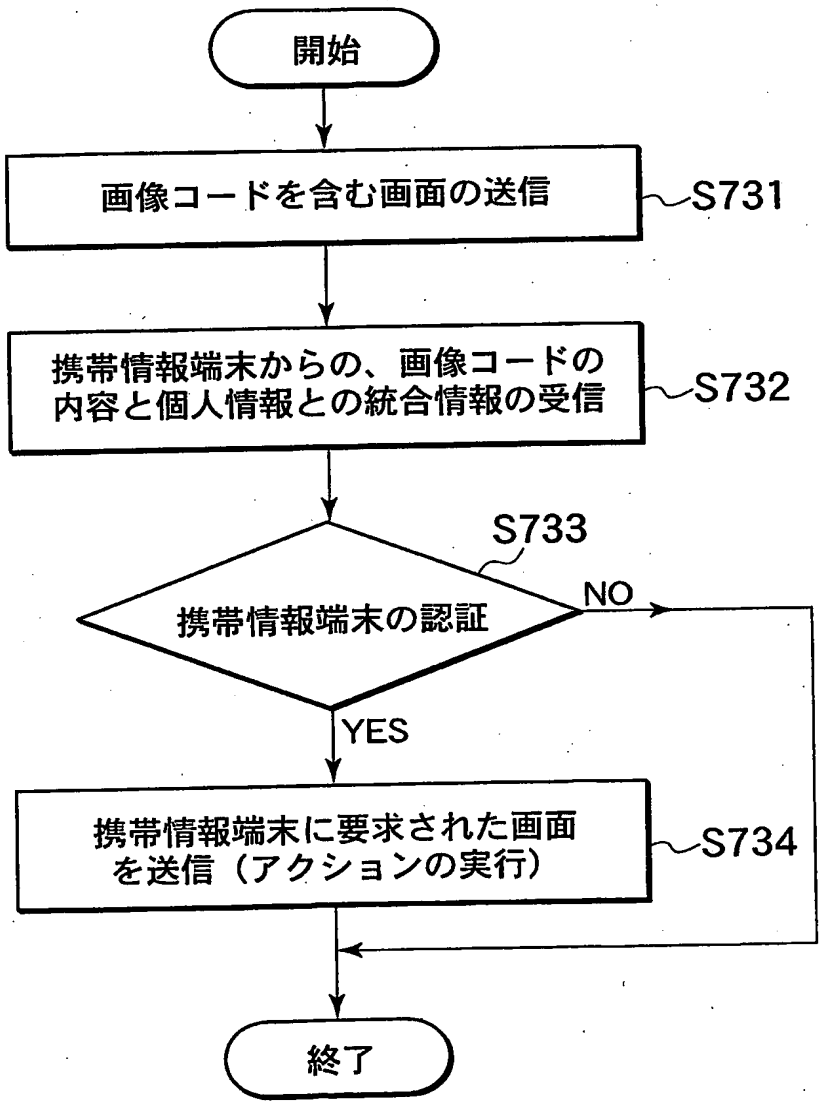

開始
画像コードを含む画面の送信
S731
携帯情報端末からの、画像コードの内容と個人情報との統合情報の受信
S732
S733
携帯情報端末の認証
NO
YES
携帯情報端末に要求された画面を送信（アクションの実行）
S734
終了

FIG. 36

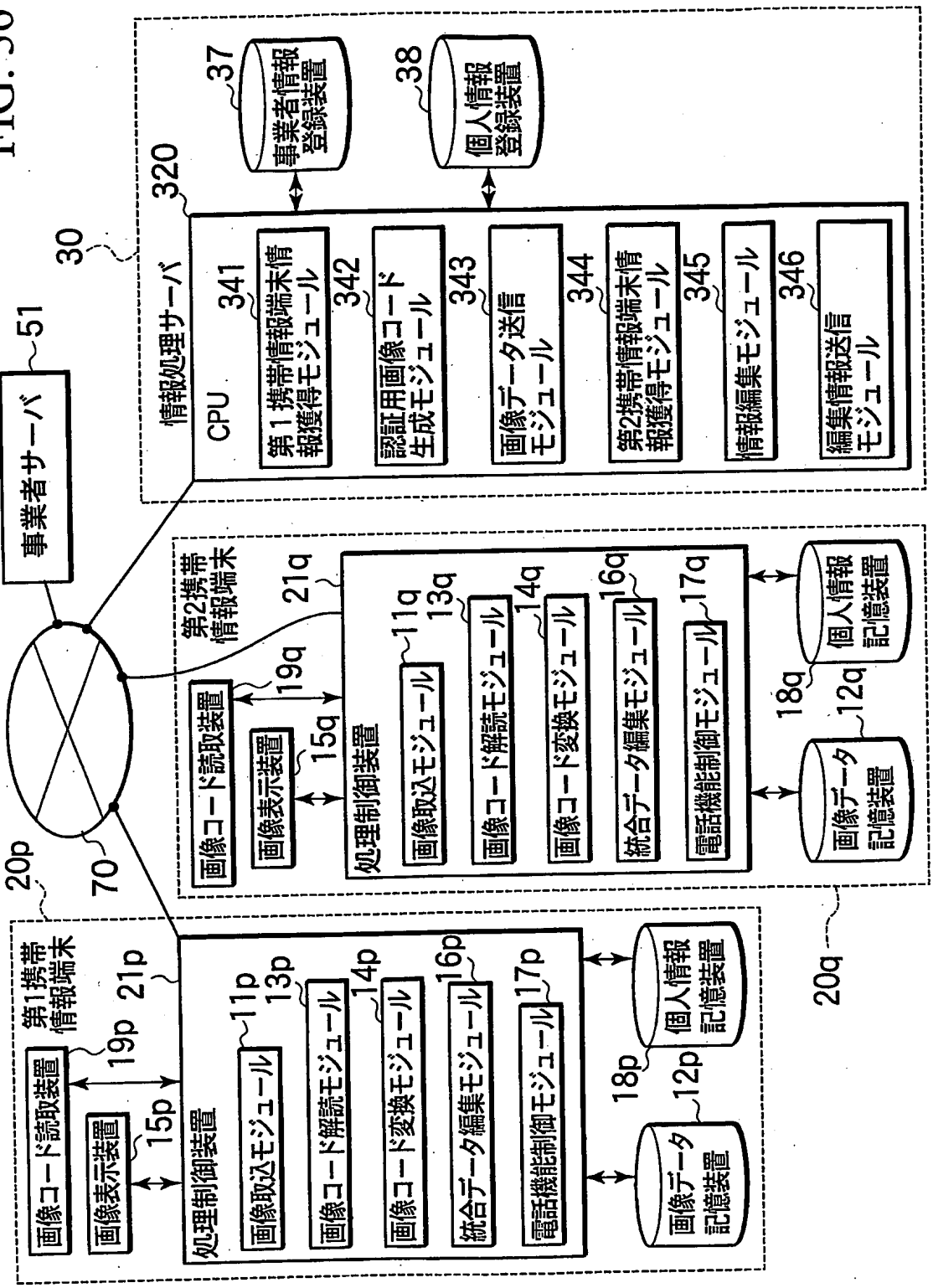

情報処理サーバ
320
CPU
341
第1携帯情報端末情報獲得モジュール
342
認証用画像コード生成モジュール
343
画像データ送信モジュール
344
第2携帯情報端末情報獲得モジュール
345
情報編集モジュール
346
編集情報送信モジュール
37
事業者情報登録装置
38
個人情報登録装置
30
事業者サーバ
51
70
第2携帯情報端末
画像コード読取装置
19q
画像表示装置
15q
処理制御装置
21q
画像取込モジュール
11q
画像コード解読モジュール
13q
画像コード変換モジュール
14q
統合データ編集モジュール
16q
電話機能制御モジュール
17q
18q
個人情報記憶装置
画像データ記憶装置
12q
20q
第1携帯情報端末
画像コード読取装置
19p
画像表示装置
15p
処理制御装置
21p
画像取込モジュール
11p
画像コード解読モジュール
13p
画像コード変換モジュール
14p
統合データ編集モジュール
16p
電話機能制御モジュール
17p
18p
個人情報記憶装置
画像データ記憶装置
12p
20p

FIG. 37

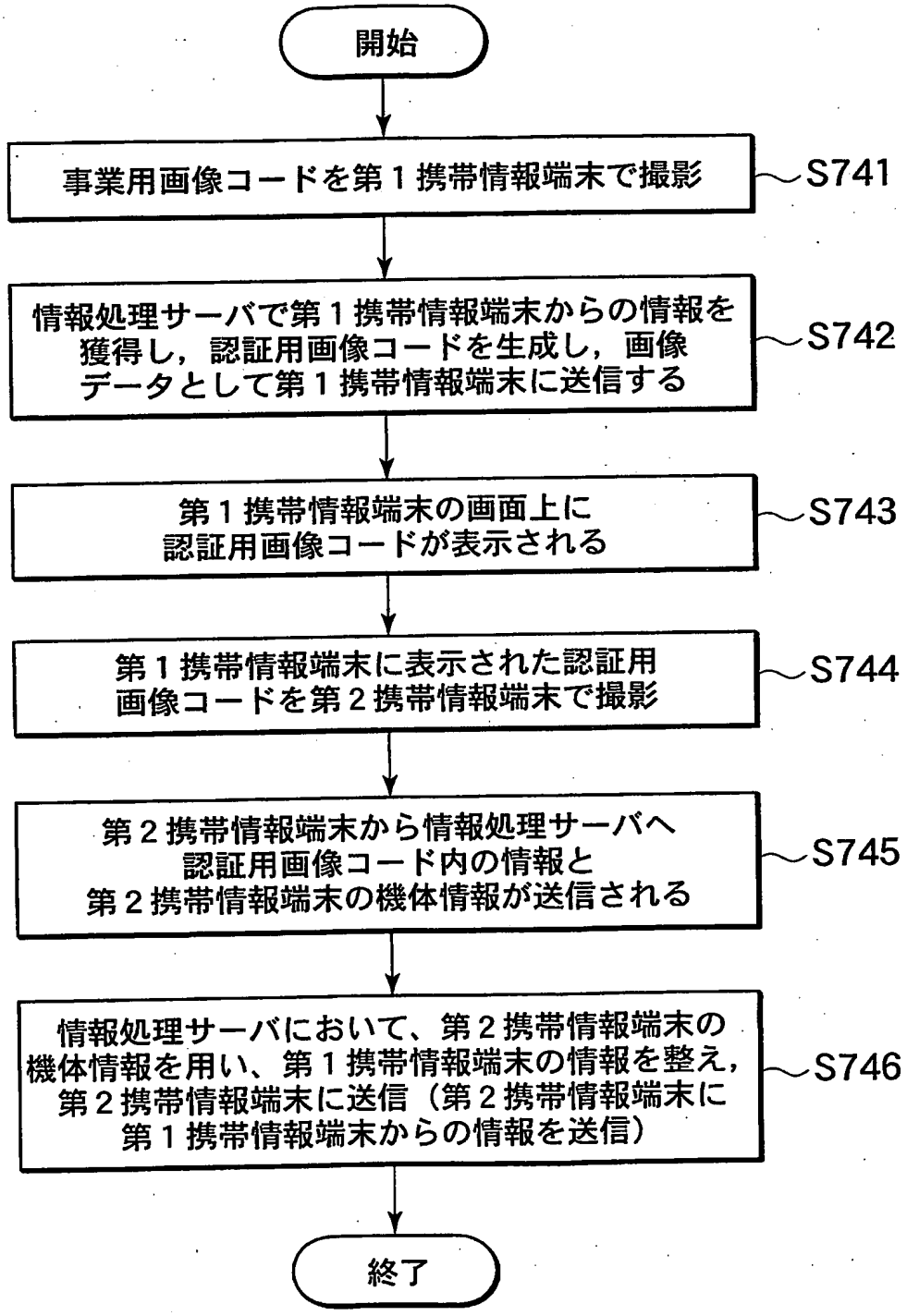

開始
事業用画像コードを第１携帯情報端末で撮影
S741
情報処理サーバで第１携帯情報端末からの情報を獲得し，認証用画像コードを生成し，画像データとして第１携帯情報端末に送信する
S742
第１携帯情報端末の画面上に認証用画像コードが表示される
S743
第１携帯情報端末に表示された認証用画像コードを第２携帯情報端末で撮影
S744
第２携帯情報端末から情報処理サーバへ認証用画像コード内の情報と第２携帯情報端末の機体情報が送信される
S745
情報処理サーバにおいて、第２携帯情報端末の機体情報を用い、第１携帯情報端末の情報を整え，第２携帯情報端末に送信（第２携帯情報端末に第１携帯情報端末からの情報を送信）
S746
終了

FIG. 38

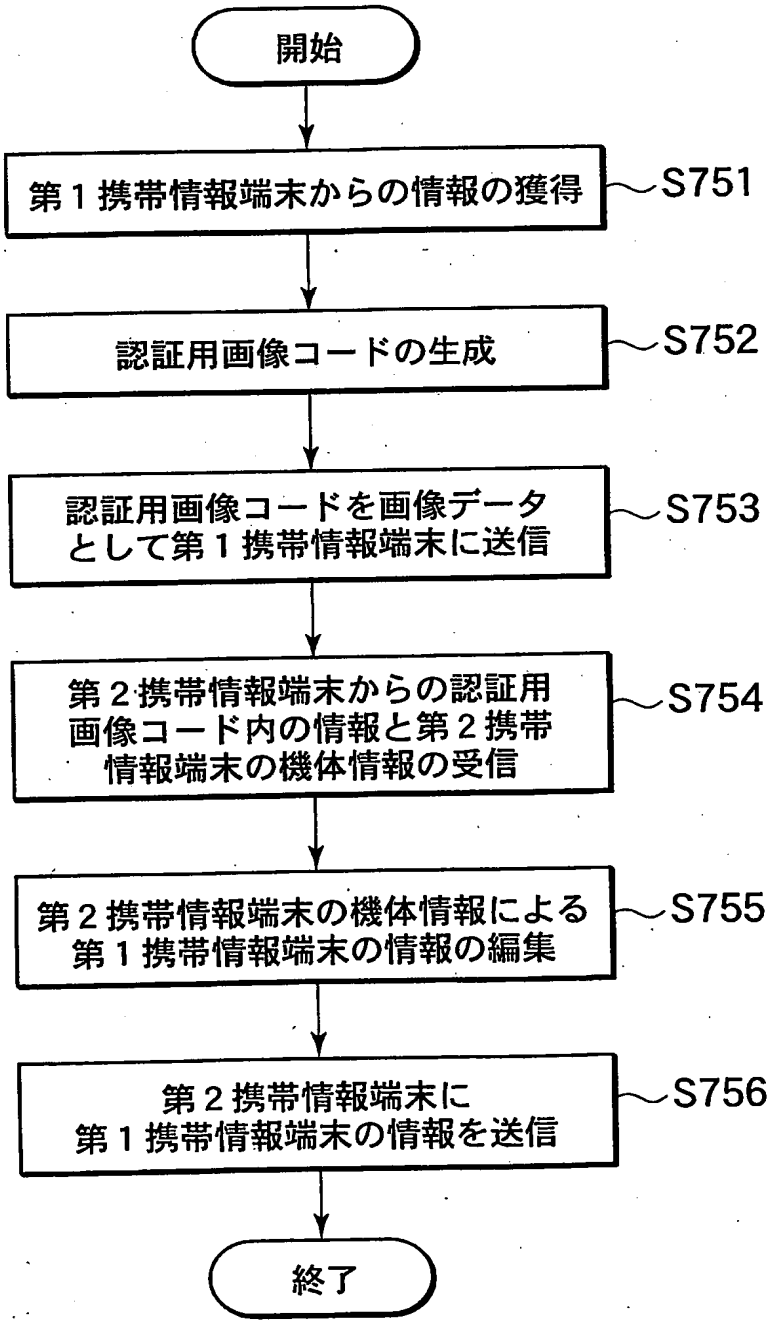

開始
第１携帯情報端末からの情報の獲得
S751
認証用画像コードの生成
S752
認証用画像コードを画像データとして第１携帯情報端末に送信
S753
第２携帯情報端末からの認証用画像コード内の情報と第２携帯情報端末の機体情報の受信
S754
第２携帯情報端末の機体情報による第１携帯情報端末の情報の編集
S755
第２携帯情報端末に第１携帯情報端末の情報を送信
S756
終了

FIG. 39

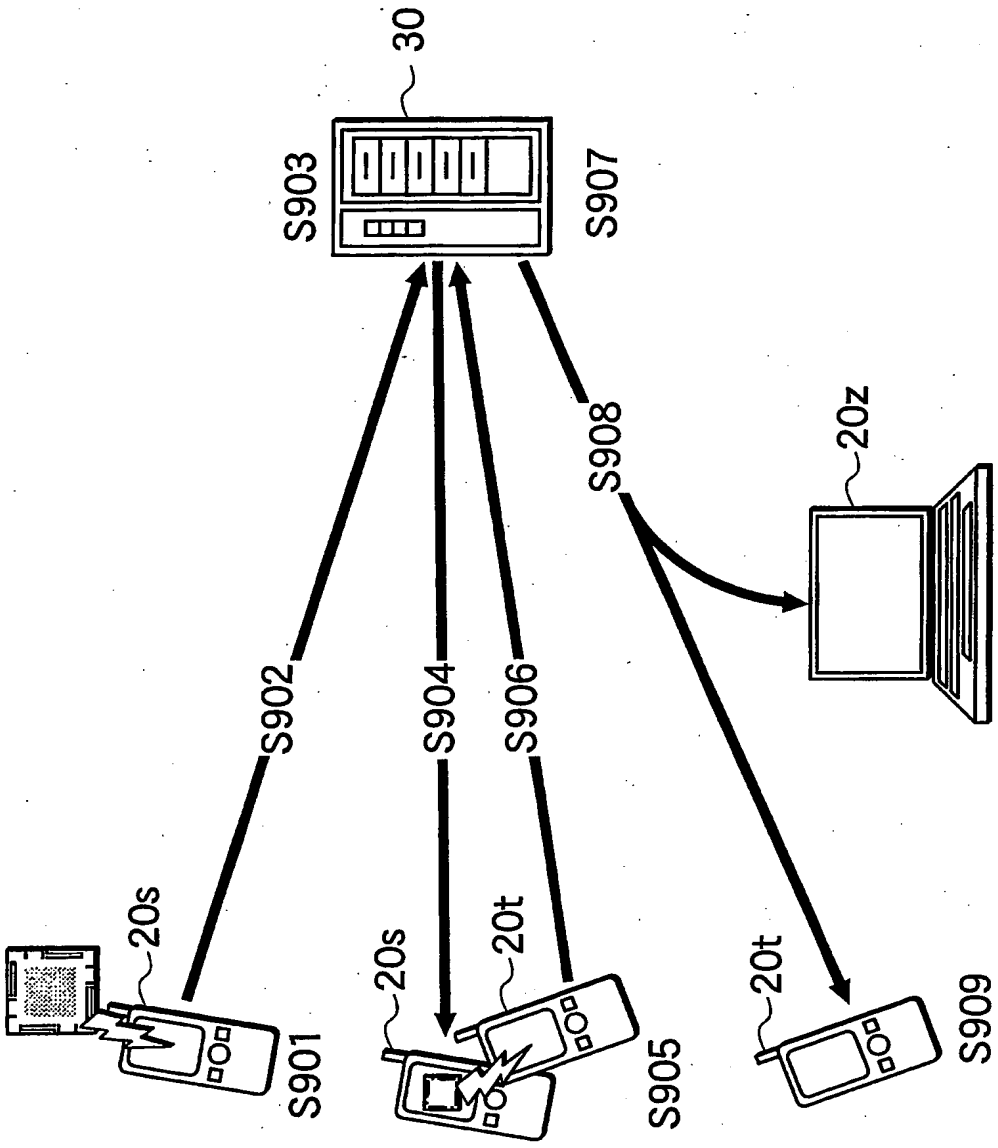

30
S903
S907
S908
20z
S902
S904
S906
20s
20t
20s
20t
S901
S905
S909

FIG. 40

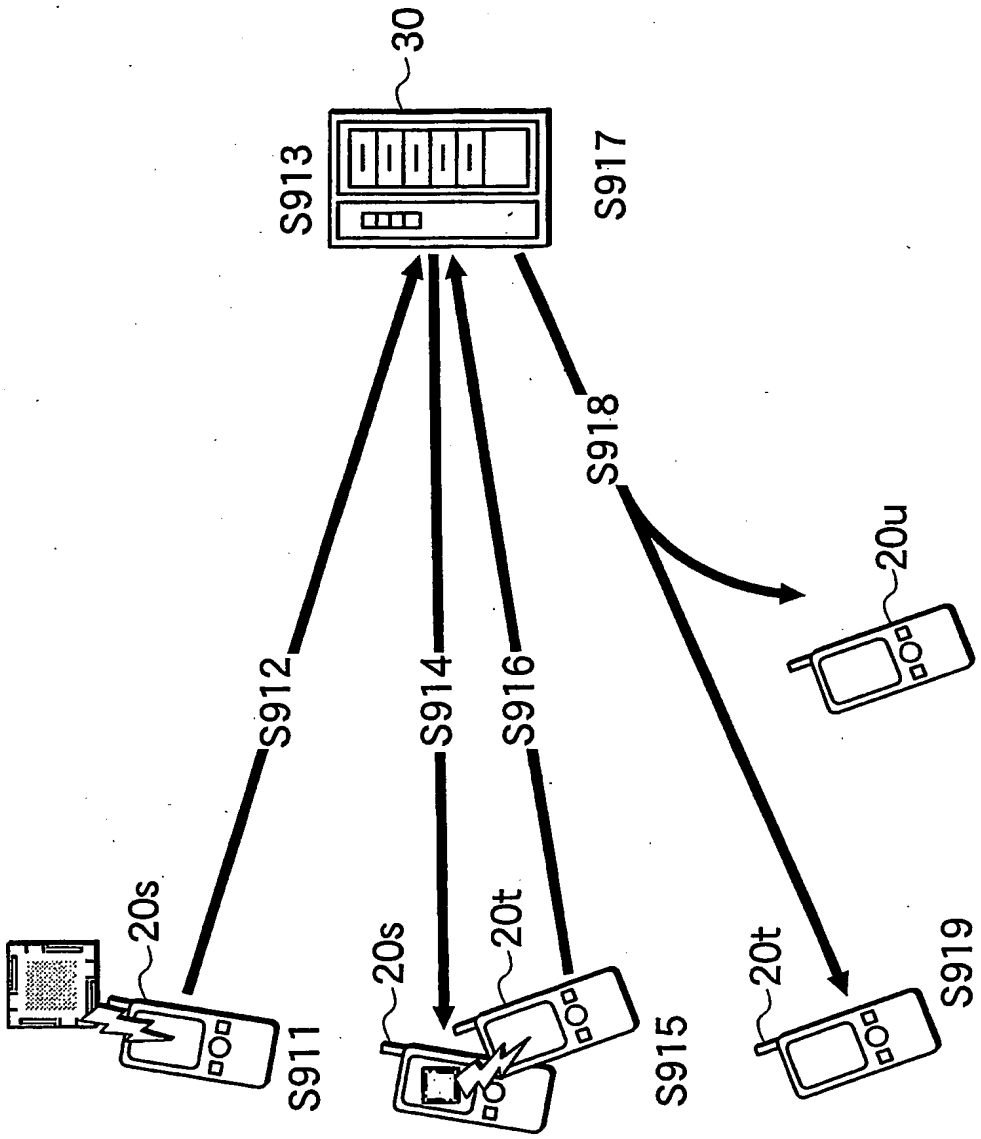
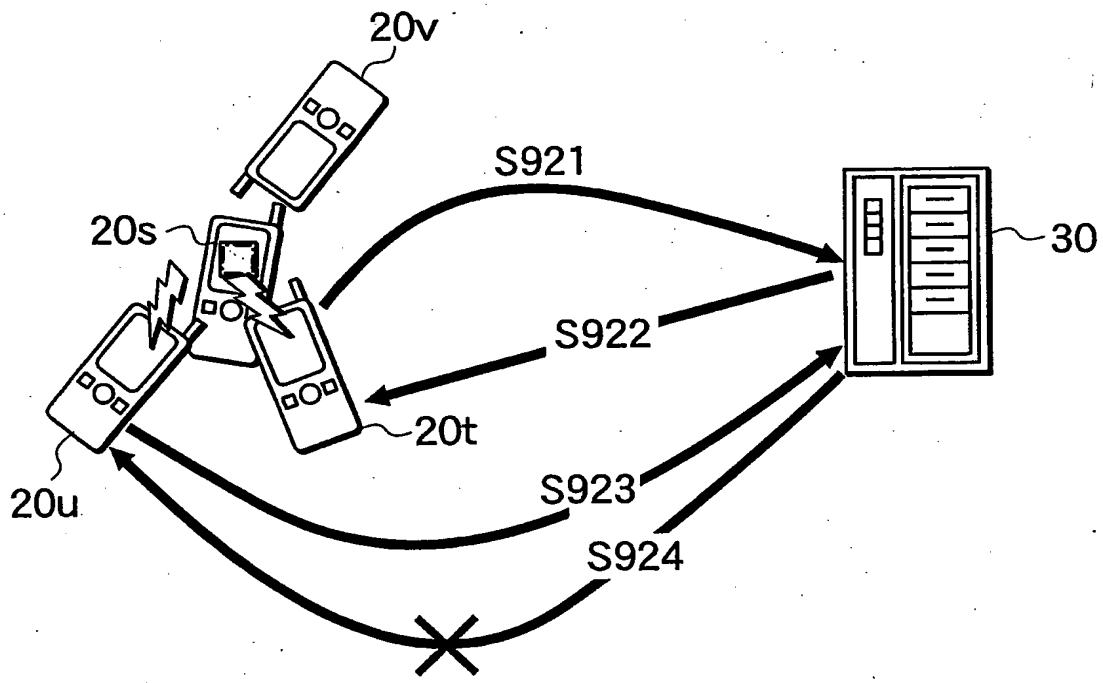

30
S913
S917
S912
S914
S916
S918
20u
20s
20s
20t
20t
S911
S915
S919

FIG. 41



INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2004/007112

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl[7] G06F15/00, H04L9/32

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
Int.Cl[7] G06F15/00, H04L9/32

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho	1922-1996	Toroku Jitsuyo Shinan Koho	1994-2004
Kokai Jitsuyo Shinan Koho	1971-2004	Jitsuyo Shinan Toroku Koho	1996-2004

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP 2002-344444 A (Sony Corp.), 29 November, 2002 (29.11.02), Full text; Figs. 1 to 27 & US 2002-184539 A	1-16
A	JP 2003-152713 A (Canon Inc.), 23 May, 2003 (23.05.03), Full text; Figs. 1 to 12 (Family: none)	1-16
X A	JP 2002-312280 A (Seiko Epson Corp.), 25 October, 2002 (25.10.02), Full text; Figs. 1 to 7 (Family: none)	17-19 20-23

☒ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search 16 August, 2004 (16.08.04)	Date of mailing of the international search report 31 August, 2004 (31.08.04)
Name and mailing address of the ISA/ Japanese Patent Office Facsimile No.	Authorized officer Telephone No.

Form PCT/ISA/210 (second sheet) (January 2004)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2004/007112

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP 2003-189020 A (Oto MATSUSHITA), 04 July, 2003 (04.07.03), Full text; Figs. 1 to 5 (Family: none)	17-23
A	JP 2001-222483 A (Sony Corp.), 17 August, 2001 (17.08.01), Full text; Figs. 1 to 14 (Family: none)	17-23

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2004/007112

Box No. II Observations where certain claims were found unsearchable (Continuation of item 2 of first sheet)

This international search report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:

2. ☐ Claims Nos.:
because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:

3. ☐ Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box No. III Observations where unity of invention is lacking (Continuation of item 3 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

The inventions of claims 1-16 relate to a technical feature that a communication terminal having no authentication information is authenticated by judging whether authentication information in the authentication terminal coincides with the authentication information stored in the authentication information storage device and transmitting the result to the communication terminal.

(Continued to extra sheet.)

1. ☒ As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.
2. ☐ As all searchable claims could be searched without effort justifying an additional fee, this Authority did not invite payment of any additional fee.
3. ☐ As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:

4. ☐ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

Remark on Protest

☐ The additional search fees were accompanied by the applicant's protest.

☒ No protest accompanied the payment of additional search fees.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2004/007112

Continuation of Box No.III of continuation of first sheet(2)

The inventions of claims 17-23 relate to a technical feature that there are provided an identifier correspondence information storage device for storing correspondence information searched by a communication terminal identifier and an information conversion module for converting the information inputted from the communication terminal, according to the correspondence information.